Cognos® 8 Business Intelligence

INSTALLATION AND CONFIGURATION GUIDE

COGNOS®

THE NEXT LEVEL OF PERFORMANCE™

Product Information

This document applies to Cognos® 8 Version 8.3 and may also apply to subsequent releases. To check for newer versions of this document, visit the Cognos Global Customer Services Web site (http://support.cognos.com).

Copyright

Copyright © 2007 Cognos Incorporated.

Portions of Cognos® software products are protected by one or more of the following U.S. Patents: 6,609,123 B1; 6,611,838 B1; 6,662,188 B1; 6,728,697 B2; 6,741,982 B2; 6,763,520 B1; 6,768,995 B2; 6,782,378 B2; 6,847,973 B2; 6,907,428 B2; 6,853,375 B2; 6,986,135 B2; 6,995,768 B2; 7,062,479 B2; 7,072,822 B2; 7,111,007 B2; 7,130,822 B1; 7,155,398 B2; 7,171,425 B2; 7,185,016 B1;7,213,199 B2.

Cognos and the Cognos logo are trademarks of Cognos Incorporated in the United States and/or other countries. All other names are trademarks or registered trademarks of their respective companies.

While every attempt has been made to ensure that the information in this document is accurate and complete, some typographical errors or technical inaccuracies may exist. Cognos does not accept responsibility for any kind of loss resulting from the use of information contained in this document.

This document shows the publication date. The information contained in this document is subject to change without notice. Any improvements or changes to either the product or the document will be documented in subsequent editions.

U.S. Government Restricted Rights. The software and accompanying materials are provided with Restricted Rights. Use, duplication, or disclosure by the Government is subject to the restrictions in subparagraph (C)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or subparagraphs (C)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48CFR52.227-19, as applicable. The Contractor is Cognos Corporation, 15 Wayside Road, Burlington, MA 01803.

This software/documentation contains proprietary information of Cognos Incorporated. All rights are reserved. Reverse engineering of this software is prohibited. No part of this software/documentation may be copied, photocopied, reproduced, stored in a retrieval system, transmitted in any form or by any means, or translated into another language without the prior written consent of Cognos Incorporated.

Table of Contents

Introduction 11

Chapter 1: What's New? 15

New Features in Version 8.3 15

Cognos 8 Transformer 15

Transformer 8.3 Installation Download 15

Series 7 IQD Bridge 16

Archive Location Property 16

Portal Services for Microsoft SharePoint 16

Support for Windows Vista 16

Changed Features in Version 8.3 16

Cognos 8 Go! Office 16

Product Behavior After Upgrade 17

Installing Transformer 17

Configuring Transformer 17

Cognos 8 Samples 18

Deprecated Features in Version 8.3 18

Configuring Content Manager 18

Configuring cogformat.xml: Notice of Intent to Change 18

Removed Features in Version 8.3 18

Smart Client Deployment for Cognos 8 Go! Office 18

Chapter 2: Components Used by Cognos 8 21

Server Components 21

Modeling Components 23

Third-party Components 24

Chapter 3: Distribution Options for Cognos 8 27

Distributing Cognos 8 Reporting Components 27

All Components on One Computer 28

Gateways on Separate Computers 29

Application Tier Components and Content Managers on Separate Computers 30

Cognos 8 Products on the Same Computer 31

Distributing Framework Manager Components 32

Distributing Transformer Components 34

Distributing Cognos 8 Scorecarding Components 37

All Components on One Computer 38

Gateways on Separate Computers 38

Application Tier Components and Content Managers on Separate Computers 39

Cognos 8 Products on the Same Computer 41

Distributing Metric Designer Components 41

Cognos 8 with Other Cognos Products 43

Cognos Products That Can Be Upgraded to Cognos 8 44

Cognos Series 7 Products That Can Be Migrated to Cognos 8 45

Cognos Products That Interoperate with Cognos 8 45
Cognos Series 7 Content That Can Be Recreated in Cognos 8 47

Chapter 4: Upgrading to Cognos 8 49
Planning the Upgrade 50
Review the Documentation 50
Conduct a Site Survey 51
Perform a Trial Upgrade 53
Review the Move to the Production Environment 53
Upgrading from Cognos Series 7 54
Upgrading from ReportNet, Metrics Manager, or Earlier Versions of Cognos 8 55
Upgrade from an Earlier Version of Cognos 8 58
Migrate Apache Derby Databases to Cognos Content Database 64
New Product, File, and Directory Names After Upgrade from ReportNet 65
Upgrade ReportNet to Cognos 8 66
Upgrading Using the Silent Configuration Option 72
Upgrade Metrics Manager to Cognos 8 72
Install or Upgrade Third-party Products 77
Run ReportNet and Cognos 8 at the Same Time 77
Manually Uninstall the ReportNet Service on Windows 79
Set Up to Publish Series 7 PowerCubes After Upgrade from ReportNet 80
Upgrading Cognos 8 Go! Office 81
Uninstall the Previous Version 81
Install Microsoft .NET Framework and the New Version of Cognos 8 Go! Office 82
Upgrading Transformer Models and PowerCubes 83
Prepare Models in Cognos Series 7 Transformer 83
Import Unsecured Models in Cognos 8 Transformer 84
Upgrade a Cognos Series 7 Secured PowerCube 85

Chapter 5: Workflows for Cognos 8 87
Installing Cognos 8 88
Single-computer Installation 88
Distributed Installation 89
Adding Framework Manager to a Cognos 8 Installation 90
Adding Metric Studio to a Cognos 8 Installation 90
Adding Transformer to a Cognos 8 Installation 92

Chapter 6: Installing Cognos 8 93
Recommendation - Review the Readme Before You Install 93
Verify System Requirements 94
Set Up Database Connectivity for the Reporting Database 96
Set Up Database Connectivity for the Content Store Database 97
Set Up Database Connectivity for the Metric Store Database 97
Review Supported Environments 98
Install Server Components 98
Install the Cognos 8 Samples 102
Default Settings for Cognos 8 104
Install Framework Manager 105
Default Settings for Framework Manager 107
Install Cognos 8 Transformer 108

Default Settings for Cognos 8 Transformer 111
Install Metric Designer 111
Default Settings for Metric Designer 113
Uninstalling Cognos 8 113
Uninstall Cognos 8 on UNIX or Linux 113
Uninstall Cognos 8 on Windows 114
Uninstall Cognos Content Database 115

Chapter 7: Setting Up the Environment 117
Create the Content Store 118
Create the Metric Store 124
Set Up the Database Client 127
Setting Up Environment Variables on UNIX for the Metric Store 130
Update the Java Environment 131
Configure the Web Server 132
Enable SSL on the Web Server 133
Configure Web Browsers 135
Configure a User Account for Cognos 8 137
Configure the Router to Test Dispatcher Availability 138
Set Up the Data Source or Import Source Environment 138
Setting Up ODBC Connections to Sybase IQ or Netezza 142

Chapter 8: Configuring Cognos 8 145
Start Cognos Configuration 145
Configuring Single Computer Installations 146
Set Database Connection Properties for the Content Store 147
Specify a Mail Server Account and Notification Database 149
Update File Location Properties 150
Start the Cognos 8 Services 151
Test the Installation and Configuration 152
Create a Metric Package 154
Finishing the Configuration 156
Configuring Distributed Installations 156
Configuring Content Manager Computers 158
Configuring Application Tier Components Computers 167
Configure Gateway Computers 171
Create a Metric Package 174
Configuring Framework Manager Computers 176
Configuring Transformer 180
Deploying Cognos 8 Transformer for Modelers 187
Configure Metric Designer 188
Start the Cognos 8 Services 191
Test the Installation and Configuration 192
Changing Default Configuration Settings 193
Change Default User and Password for Cognos Content Database 194
Change a URI 196
Configure Cryptographic Settings 199
Configure Cognos 8 Components to Use Cognos Application Firewall 201
Configure Temporary File Properties 202
Configure the Gateway to Use a Namespace 203

Enable and Disable Services 203
Specify Resources for the Cognos 8 Service 204
Configuring Fonts 205
Change the Default Font for PDF Reports 207
Configure Embedded Fonts for PDF Reports 208
Saved Report Output 209
Change the Location of Map Charts for Report Studio 210
Configuring the SSL Protocol 211
Configure SSL for Cognos 8 211
Set Up Shared Trust Between Cognos Servers and Other Servers 213
Select and Rank Cipher Suites for SSL 214
Configuring Log Messages 215
Log Message Destinations 216
Set Up the Database Client for a Logging Database 217
Specify the Log Messages Destination 219
Changing Global Settings 221
Customize Language Support to the User Interface 221
Customizing Currency Support 222
Customize Content Locale Support 224
Map Content Locales 225
Map Product Locales 227
Customize the Server Time Zone 228
Change Encoding for Email Messages 228
Customize Cookie Settings 230
Changing the Gateway 231
Configure the Gateway for Cognos Apache Web Server Module 231
Configure the Servlet Gateway 233
Configuring Cognos 8 to Work with Other Cognos Products 234
Enable Scheduled Reports and Agents for Cognos Planning Contributor Data Sources 234

Chapter 9: Configuring Cognos 8 Go! Office 237
Create a Virtual Directory for Cognos 8 Go! Office 237
Update the Recognized Content Types for the Web Server 238
Enable SSL Support for the HTTPS Interface to PowerPlay 239
Enable Anonymous Access for PowerPlay 240
Deploying Cognos 8 Go! Office Client 240
Install Microsoft .NET Framework and Cognos 8 Go! Office 240
Set Macro Security Level for Microsoft Office XP 242
Test Cognos 8 Go! Office 242

Chapter 10: Configuring Portal Services 243
Specify the Location of the Applications.xml File 243
Configuring Security for Portal Services 244
Disable Anonymous Access to Cognos 8 Components 244
Enable Single Signon Using Shared Secret 245
Enable Single Signon for SAP EP with the SAP Logon Ticket 250
Enable Single Signon for SAP EP with User Mapping 251
Enable Secure Communication Between SAP EP and Cognos 8 Components 252
Enable Single Signon for WebSphere Portal Using the Application Server 252
Enable Single Signon for Plumtree Portal Using Basic Authentication 253

Enable Single Signon for Plumtree Portal Using SiteMinder 253

Chapter 11: Configuring Cognos 8 Components to Use an Authentication Provider 255

Disable Anonymous Access 256
Restrict User Access to the Cognos Namespace 257
Configuring Cognos 8 Components to Use Active Directory Server 257
Configure an Active Directory Namespace 258
Make Custom User Properties for Active Directory Available to Cognos 8 Components 259
Enabling Secure Communication to the Active Directory Server 260
Include or Exclude Domains Using Advanced Properties 261
Enabling Single Signon Between Active Directory Server and Cognos 8 Components 262
Configuring Cognos 8 to Use Cognos Series 7 Namespace 263
Configure a Cognos Series 7 Namespace 263
Enabling Secure Communication to the Directory Server Used by the Series 7 Namespace 264
Enabling Single Signon Between Cognos Series 7 and Cognos 8 265
Cognos Series 7 Namespaces and the Cognos Series 7 Trusted Signon Plug-in 265
Configuring Cognos 8 to Use a Custom Authentication Provider 268
Configure a Custom Authentication Namespace 268
Configuring Cognos 8 Components to Use LDAP 268
Configure an LDAP Namespace 269
Configure an LDAP Namespace for Active Directory Server 271
Configure an LDAP Namespace for IBM Directory Server 273
Configure an LDAP Namespace for Novell Directory Server 275
Configure an LDAP Namespace for Sun Java System Directory Server 278
Make Custom User Properties for LDAP Available to Cognos 8 Components 280
Enable Secure Communication to the LDAP Server 281
Enabling Single Signon Between LDAP and Cognos 8 Components 282
Replace Operation 283
Configuring Cognos 8 Components to Use eTrust SiteMinder 283
Configure a Netegrity SiteMinder Namespace 285
Enabling Secure Communication to the eTrust SiteMinder User Directory 286
Enable Single Signon Between eTrust SiteMinder and Cognos 8 286
Protecting the Cognos Web Alias 286
Configuring Cognos 8 Components to Use an NTLM Namespace 286
Configure an NTLM Namespace 287
Enable Single Signon Between NTLM and Cognos 8 Components 287
Configuring Cognos 8 to Use SAP 288
Configure an SAP Namespace 289
Enable Single Signon Between SAP and Cognos 8 290
Test the Namespaces 291
Delete an Authentication Provider 291

Chapter 12: Configuring Cognos 8 for a Third-Party Application Server 293

Create a Separate JVM Instance 294
Check the Setup of Cognos Components 295
Back Up Existing Cognos Information 295
Set Environment Variables 297
Update the Java Environment 298
Configure Cognos Components to Run Within the Application Server 298
Identifying the JDK for WebLogic 9 on AIX 300

Change the Application Server Startup Script 301
Change the Cognos Dispatcher Properties File for Oracle Application Server 303
Configure Application Server Properties and Deploy Cognos Components 303
Enable SSL 310
Configuring the Web Server 310
Unregister Dispatchers 310
Import Content Store Data 311
Upgrade to Cognos 8 in an Application Server Environment 311
Upgrade from Metrics Manager to Cognos 8 in an Application Server Environment 312

Chapter 13: Advanced Configuration Options 313
Change the Type of JVM Used by Cognos 8 313
Changing the Version of Java Runtime Environment Used by Cognos 8 Components 314
Back Up Existing Cognos Information 314
Update the Java Environment 316
Import Content Store Data 317
Configuring Cognos 8 Components to Use a Third-party Certificate Authority 317
Generate Keys and Certificate Signing Requests 317
Configure Cognos 8 Components to Run Within a Third-party Certificate Authority 321

Chapter 14: Samples 323
Great Outdoors Samples 323
The Great Outdoors Group of Companies 324
Employees 325
Sales and Marketing 325
Great Outdoors Database, Models, and Packages 326
Setting Up the Samples 328
Restore Backup Files for the Samples Databases 329
Create Data Source Connections to the Samples Databases 330
Set Up Microsoft Analysis Services Cube Samples 332
Set Up the DB2 Cube Sample 332
Create Data Source Connections to OLAP Data Sources 333
Set Up the Metric Studio Sample 335
Import the Samples 336
Sample Database Models 338
Example - Running the Sample ELM Returns Agent Against Changed Data 339
Remove the Samples Databases from Cognos 8 341

Chapter 15: Setting Up an Unattended Installation and Configuration 343
Set Up an Unattended Installation 343
Set Up an Unattended Configuration 346

Chapter 16: Performance Maintenance 349
System Performance Metrics 349
Enabling Only Services That are Required 349
Tuning a DB2 Content Store 352
Tune Apache Tomcat Settings 352
Increase the Request-handling Capacity for Cognos Content Database 353
Improve Metric Store Database Performance 353
Reduce Delivery Time for Reports in a Network 354

Appendix A: Manually Configuring Cognos 8 *355*
Manually Configuring Cognos 8 on UNIX and Linux *355*
Manually Change Default Configuration Settings on UNIX and Linux Computers *356*
Manually Change the Global Settings on UNIX and Linux Computers *359*
Starting and Stopping Cognos 8 in Silent Mode on UNIX and Linux Computers *360*
Manually Create a Cognos Application File *361*

Appendix B: Troubleshooting *365*
Log Files *365*
Problems Starting Cognos 8 *367*
CFG-ERR-0106 Error When Starting the Cognos 8 Service in Cognos Configuration *368*
Unable to Start the Cognos 8 Service Because the Port is Used by Another Process *369*
Cognos 8 Service Does Not Start or Fails After Starting *370*
Cognos 8 Server Fails to Start and Gives No Error Message *371*
Cognos BI Server Not Available When Starting Cognos 8 *371*
Cannot Log On to a Namespace When Using Cognos Connection (PRS-CSE-1255 Error) *375*
Cognos 8 Services Fail to Restart After a Network Outage *375*
No Warning That Installing a Later Version of Cognos 8 Will Automatically Update the Earlier Version of the Content Store *376*
Download of Resource Fails *376*
DB2 Returns SQL1224N Error When Connecting from AIX *376*
Content Manager Error When Starting Cognos 8 *376*
Cannot Open an MS Cube or PowerCube *377*
Cannot Open an OLAP Data Source *378*
The Page Cannot Be Found When Starting Cognos 8 in Windows 2003 *378*
The Page Is Not Shown When Opening a Portal After Installing Cognos 8 *378*
DPR-ERR-2058 Error Appears in Web Browser When Starting Cognos 8 *378*
EBA-090034 Error When Starting WebLogic 8 *380*
Report Studio Does Not Start *381*
DPR-ERR-2022 Error Appears in Web Browser When Starting Cognos 8 *381*
Unable to Download the cognos.xts File *381*
Application Server Startup Script Fails *382*
Deploying Cognos 8 to an Oracle Application Server or IBM WebSphere Application Server Fails *382*
Microsoft Excel 2000 Multipage Report Type Does Not Work *383*
Unable to Deserialize Context Attribute Error When Deploying the p2pd.war File to WebLogic *383*
Error Appears After Upgrading Cognos 8 on a WebLogic Application Server *384*
Chinese, Japanese, or Korean Characters Are Different After Upgrade *384*
Accented or Double-Byte Characters May Not Display Correctly When Installing Cognos 8 on Linux *385*
Problems Configuring Cognos 8 *385*
Run Database Cleanup Scripts *385*
Error Trying to Encrypt Information When Saving Your Configuration *387*
Problems Generating Cryptographic Keys in Cognos Configuration *388*
CAM-CRP-1315 Error When Saving Configuration *388*
Configuration Data is Locked by Another Instance of Cognos Configuration *389*
Unable to Exit a Tab Sequence When Using Keyboard-only Navigation in Cognos Configuration *389*

Unable to Save Your Configuration *389*
Java Error When Starting Cognos Configuration *390*
Cryptographic Error When Starting Cognos Configuration *390*
Current Configuration Settings Are Not Applied to Your Computer *391*
CM-CFG-029 Error When Trying to Save a Configuration That Specifies a SQL Server Data Source *391*
Users are Prompted for Active Directory Credentials *391*
Font on UNIX Not Found When Starting Cognos Configuration *392*
Unable to Load DB2 OLAP Library in Framework Manager *392*
Group Membership is Missing From Active Directory Namespace *393*
Deploying Cognos 8 to an Oracle Application Server or IBM WebSphere Application Server *394*
Errors Displayed Deploying to Oracle 10G Application Server *394*
Page Cannot be Found Error Running Reports using Cognos 8 Go! Office *394*
Error Initializing Oracle Content Store After Upgrade from ReportNet *395*
CGI Timeout Error While Connected to Cognos 8 Components Through a Web Browser *395*
Servlet Class Fails to Load in WebLogic *396*
Desktop Icons or Cognos Configuration Window Flicker on Windows *397*

Glossary *399*

Index *405*

Introduction

This document is intended for use with Cognos 8. Cognos 8 is a Web product with integrated reporting, analysis, scorecarding, and event management features.

This guide contains instructions for installing, upgrading, configuring, and testing Cognos 8, changing application servers, and setting up samples.

Audience

To use this guide, you should be familiar with

- reporting concepts
- scorecarding concepts
- database and data warehouse concepts
- security issues
- basic Windows and/or UNIX administration skills
- the existing server environment and security infrastructure in your organization

Related Documentation

Our documentation includes user guides, getting started guides, new features guides, readmes, and other materials to meet the needs of our varied audience. The following documents contain related information and may be referred to in this document.

Note: For online users of this document, a Web page such as **The page cannot be found** may appear when clicking individual links in the following table. Documents are made available for your particular installation and translation configuration. If a link is unavailable, you can access the document on the Cognos Global Customer Services Web site (http://support.cognos.com). Logon credentials are available either from your administrator or by request from support.america@cognos.com.

Document	Description
Cognos 8 Administration and Security Guide	Managing servers, security, reports, and portal services; setting up Cognos samples; troubleshooting; and customizing Cognos 8
Cognos Configuration User Guide	Using Cognos Configuration to configure Cognos 8

Document	Description
Cognos 8 Architecture and Deployment Guide	Understanding the Cognos 8 architecture, developing installation strategies, including security considerations, and optimizing performance
Framework Manager User Guide	Creating and publishing models using Framework Manager
Metric Studio User Guide	Authoring scorecard applications and monitoring the metrics within them
Metric Designer User Guide	Creating extracts that map and transfer information from relational and dimensional data sources to Metric Studio
Cognos 8 Go! Office User Guide	Using Cognos 8 Go! Office to retrieve content from Cognos reporting products within Microsoft Office
Cognos 8 Transformer User Guide	Modeling and building PowerCubes using Model Definition Language (MDL) scripts
Cognos 8 and Composite Information Server *Getting Started*	Installing, configuring, and using Composite Information Server with Cognos 8 and Framework Manager; provides access to distributed information sources

Finding Information

To find the most current product documentation, including all localized documentation, access the Cognos Global Customer Services Web site (http://support.cognos.com). Click the **Documentation** link to access documentation guides. Click the **Knowledge Base** link to access all documentation, technical papers, and multimedia materials.

Product documentation is available in online help from the **Help** menu or button in Cognos products. You can also download documentation in PDF format from the Cognos Global Customer Services Web site.

You can also read PDF versions of the product readme files and installation guides directly from Cognos product CDs.

Using Quick Tours

Quick tours are short online tutorials that illustrate key features in Cognos product components. To view a quick tour, start Cognos Connection and click the **Quick Tour** link in the lower-right corner of the Welcome page.

Getting Help

For more information about using this product or for technical assistance, visit the Cognos Global Customer Services Web site (http://support.cognos.com). This site provides product information, services, user forums, and a knowledge base of documentation and multimedia materials. To create a case, contact a support person, or to provide feedback, click the **Contact Us** link. For information about education and training, click the **Training** link.

Printing Copyright Material

You can print selected pages, a section, or the whole book. Cognos grants you a non-exclusive, non-transferable license to use, copy, and reproduce the copyright materials, in printed or electronic format, solely for the purpose of operating, maintaining, and providing internal training on Cognos software.

Chapter 1: What's New?

This section contains a list of new, changed, deprecated, and removed features for this release. It will help you plan your upgrade and application deployment strategies and the training requirements for your users.

For information about upgrading, see the *Installation and Configuration Guide* for your product.

For information about new features for this release, see the *New Features Guide*.

To review an up-to-date list of environments supported by Cognos products, such as operating systems, patches, browsers, Web servers, directory servers, database servers, and application servers, visit the Cognos support Web site (http://support.cognos.com).

New Features in Version 8.3

Listed below are new features since the last release. Links to directly-related topics are included.

Cognos 8 Transformer

Cognos Series 7 Transformer is now fully integrated with Cognos 8. You can install this optional component in your Cognos 8 environment. It offers all the features of Cognos Series 7 Transformer, and it supports user authentication and logon using supported Cognos 8 security providers. Transformer runs on all supported Cognos 8 platforms, including Linux, HP/UX Itanium, and Windows Vista. For more information, see "Install Cognos 8 Transformer" (p. 108).

You can import metadata, which includes the associated filters and prompts, from Cognos 8 packages and reports for use as a data source in Transformer 8.3. For more information, see the topic about creating a new model in the Cognos 8 Transformer *User Guide*.

Secured cubes created in Transformer 8.3 are intended for the Cognos 8 Business Intelligence Web studios and are not compatible with Cognos Series 7.x PowerPlay products.

Unsecured and password-protected PowerCubes built in Transformer 8.3 can be accessed in Cognos 8.3 Mobile Analysis for local (disconnected) use.

Transformer 8.3 supports UTF-8 encodings. Although you can use UTF-8 as a model setting when building PowerCubes, Transformer 8.3 does not support multilingual PowerCubes. Modelers must also be aware of differences between content locale in saved reports and the locale that Transformer uses when accessing reports to build PowerCubes. For more information about managing languages and locales in Transformer, see the Transformer *User Guide*.

Transformer 8.3 Installation Download

Transformer can now be made available more easily for business specialists who want to design models and build PowerCubes for their own use. For example, IT departments can provide business specialists or Transformer modelers with a Web-based, downloadable installation program from

a corporate or secured portal, allowing for easy distribution of the installation files. For more information, see "Create a Network Installation Location for Transformer Modelers" (p. 185) and "Deploying Cognos 8 Transformer for Modelers" (p. 187).

Series 7 IQD Bridge

Cognos 8 Business Intelligence Transformer uses the Cognos 8 query engine to support the features in Cognos 8. The Series 7 IQD Bridge component enables Transformer 8.3 to continue to support Cognos Series 7 .iqd files, whether the files were authored in Cognos Series 7 Impromptu, or in Cognos 8 Framework Manager as externalized queries. To use an .iqd data source with Transformer 8.3, install the Series 7 IQD Bridge on each Transformer computer that requires access to this data source type.

The Series 7 IQDBridge is an optional component and is not supported on new platforms such as Linux or HP-UX Itanium. For more information, see "Install Cognos 8 Transformer" (p. 108).

Archive Location Property

In older versions of Cognos 8, report output was saved by default in the content store. You can now configure two additional save locations, one inside Cognos 8 and one outside Cognos 8. For more information, see "Saved Report Output" (p. 209).

Portal Services for Microsoft SharePoint

Cognos 8 now supports Cognos Portlets inside the Microsoft SharePoint portal. If you want to use this feature, you must configure security after deploying the portlets in the SharePoint portal. For more information, see "Configuring Portal Services" (p. 243).

Support for Windows Vista

Cognos 8 is supported on Windows Vista. With Windows Vista, Microsoft introduced security enhancements to further protect the Program Files directory. This necessitated changes to environment variables and the directories where user profiles are stored. For more information, see "Operating Systems" (p. 58) and "Update File Location Properties" (p. 150).

Changed Features in Version 8.3

Listed below are changes to features since the last release. Links to directly-related topics are included.

Cognos 8 Go! Office

In the previous release, the installation wizard showed the name Cognos 8 Go! Office and used a default installation directory of Cognos Office. In the new release, the installation wizard shows the name Cognos 8 for Microsoft Office and uses the default installation directory of Cognos 8 for

Microsoft Office. The wizard is used for a family of Cognos products that work with Microsoft Office. For more information, see "Deploying Cognos 8 Go! Office Client" (p. 240).

In the previous release, you could configure security for Microsoft .NET Framework using a Smart client or a COM add-in. Cognos 8 Go! Office now use the COM add-in only, and no action is required to configure it. In addition, the previous release required that you set custom properties in Microsoft Office templates. In the new release, the custom properties are no longer required. For more information, see "Configuring Cognos 8 Go! Office" (p. 237).

Product Behavior After Upgrade

When you upgrade from Cognos 8 BI version 8.2 to version 8.3, some features in Cognos 8 may behave differently after the upgrade. When you upgrade reports, for example, changes in behavior may cause validation errors. Documentation is available about the behavior changes. This documentation includes examples of the changed behavior and solutions for issues that may occur during the upgrade. For more information, see *Upgrading to Cognos 8 BI 8.3: Changes in Product Behavior* on the Global Customer Services Web site (http://support.cognos.com/go/docs/cognos8_bi/8.3/changes_productbehavior.html).

Installing Transformer

In previous releases, you could not install Cognos Series 7 Transformer and Cognos 8 Transformer 7.x on the same computer. With Cognos 8 Transformer 8.3, you can install it on a computer that has Cognos Series 7 Transformer, with no conflicts.

In previous releases of Transformer, the installation location was a cer*n* directory, where *n* represented the Transformer 7.x rendition number. The Transformer 8.3 installation location is the same c8 directory used by all other Cognos 8 products.

The Transformer 8.3 executable name (on Windows and UNIX) and .ini file names are now cogtr.

Note: When Transformer 8.3 is installed on Windows Vista, if you do not have Administrator privileges on the computer and you make changes to the cogtr.xml file, the updated file is saved by default to a Virtual Store directory and not to the *c8_location*/configuration directory.

Model-, PowerCube- and Log files for Transformer 8.3 are maintained in the ..\My Documents\Transformer\ directory, in an appropriate subdirectory. Data Source and Temp file directories are stored in the default locations that are specified in Cognos Configuration. To store them in a separate location, you can specify new locations in Transformer.

For more information, see "Install Cognos 8 Transformer" (p. 108).

Configuring Transformer

Unlike previous versions of Transformer, which used Cognos Series 7 Configuration Manager, Transformer 8.3 uses Cognos Configuration for product configuration. This allows for complete integration with all Cognos 8 Business Intelligence products.

For more information, see "Configure Cognos 8 Transformer Computers" (p. 181).

Cognos 8 Samples

In previous versions of Cognos 8, the samples were installed automatically with the server components. Now the samples are on a separate CD in your Cognos 8 product. If you want to use the samples, you must install them from the Cognos 8 Business Intelligence Samples 8.3 CD. For more information, see "Install the Cognos 8 Samples" (p. 102).

Deprecated Features in Version 8.3

A deprecated feature is one that is being replaced by a newer version or a better implementation. Cognos intends to discontinue the use of the feature and provides recommendations for adapting to this change over multiple releases.

Listed below are deprecated features, including links to related topics.

Configuring Content Manager

The Create symmetric key store property could be enabled or disabled in older versions. It was typically set to true on the active Content Manager and false on standby Content Managers. These settings enabled standby Content Managers to retrieve the master common symmetric key from the active Content Manager.

The Create symmetric key store property is deprecated in Version 8.3 because Content Managers can now dynamically determine the active Content Manager and automatically retrieve the key. For more information, see "Configuring Content Manager Computers" (p. 158).

Configuring cogformat.xml: Notice of Intent to Change

Currently, configuring the cogformat.xml file location and format specification properties is done at installation time. The information is saved to a configuration file on the local computer and the configuration file is preserved when you upgrade. In the next release, configuring the cogformat.xml file location and format specification properties will be done in Cognos Administration. The properties will be stored in the content store and available to all groups and roles. To prepare for this change, you must create a backup of any customizations you made to this file. For more information about backing up files that contain customization, see "Upgrade from an Earlier Version of Cognos 8" (p. 58).

Removed Features in Version 8.3

Listed below are features that are removed since the last release. Links to directly-related topics are included.

Smart Client Deployment for Cognos 8 Go! Office

Cognos 8 Go! Office deployment no longer supports the smart client. You must use the COM add-in client, which requires that an installation be run on user computers. If Cognos Office

Connection is upgraded with a later release, COM add-in users must install the newer version. For more information about deploying Cognos GO! Office, see "Configuring Cognos 8 Go! Office" (p. 237).

Chapter 2: Components Used by Cognos 8

Cognos 8 is a Web-based business intelligence solution with integrated reporting, analysis, scorecarding, and event management features. Cognos 8 includes Cognos 8 Business Intelligence Server and Cognos 8 Business Intelligence Modeling.

Cognos 8 integrates easily into your existing infrastructure by using resources that are in your environment. Some of these existing resources are required, such as a Java Virtual Machine for UNIX installations. Other resources are optional, such as using a third-party database for the content store or a third-party security provider for authentication.

By default, Cognos 8 uses Tomcat as an application server. You can configure Cognos 8 products to run on supported application servers that you currently use in your environment.

Server Components

Server components provide the user interfaces for reporting, analysis, scorecarding, and event management, as well as the server functionality for routing and processing user requests. Server components include the following tools:

Cognos Connection

Cognos Connection is a Web portal provided with Cognos 8, providing a single access point to the corporate data available for its products. It provides a single point of entry for querying, analyzing, and organizing data, and for creating reports, scorecards, and events. Users can run all their Web-based Cognos 8 applications through Cognos Connection. Other business intelligence applications, and URLs to other applications, can be integrated with Cognos Connection.

Cognos Administration

Cognos Administration is a central management interface that contains the administrative tasks for Cognos 8. It provides easy access to the overall management of the Cognos environment and is accessible through Cognos Connection.

Cognos Viewer

Cognos Viewer is a portlet in which you can view and interact with any type of published Cognos content. It is accessible through Cognos Connection and any existing enterprise portal.

Report Studio

Report Studio lets report authors create, edit, and distribute a wide range of professional reports. They can also define corporate-standard report templates for use in Query Studio, and edit and modify reports created in Query Studio or Analysis Studio.

Query Studio

Query Studio lets users with little or no training quickly design, create and save reports to meet reporting needs not covered by the standard, professional reports created in Report Studio.

Analysis Studio

In Analysis Studio, users can explore, analyze, and compare dimensional data. Analysis Studio provides access to dimensional, OLAP (online analytical processing), and dimensionally modeled relational data sources. Analyses created in Analysis Studio can be opened in Report Studio and used to build professional reports.

Event Studio

In Event Studio, you set up agents to monitor your data and perform tasks when business events or exceptional conditions occur in your data that must be dealt with. When an event occurs, people are alerted to take action. Agents can publish details to the portal, deliver alerts by email, run and distribute reports based on events, and monitor the status of events. For example, a support call from a key customer or the cancellation of a large order may trigger an event, sending an email to the appropriate people.

Metric Studio

In Metric Studio, you can create and deliver a customized scorecarding environment for monitoring and analyzing metrics throughout your organization. Users can monitor, analyze, and report on time-critical information by using scorecards based on cross-functional metrics.

Cognos 8 Go! Office

Cognos 8 Go! Office allows Microsoft Office users to access data from Cognos reporting products within Microsoft Office applications.

Cognos 8 Go! Office components are automatically installed with Cognos 8.

Cognos 8 Go! Office is not installed with Cognos 8 Metrics Manager.

Cognos Configuration

Cognos Configuration is a tool that you use to configure Cognos 8, and to start and stop its services.

Gateway

Web communication in Cognos 8 is typically through gateways, which reside on one or more Web servers. A gateway is an extension of a Web server program that transfers information from the Web server to another server.

Gateways are often CGI programs, but may follow other standards, such as Internet Server Application Program Interface (ISAPI) and Apache Modules (apache_mod).

Content Manager

Content Manager is the Cognos 8 service that manages the storage of customer application data, including security, configuration data, models, metrics, report specifications, and report output.

Content Manager is needed to publish models, retrieve or store report specifications, manage scheduling information, and manage the Cognos namespace.

Content Manager stores information in a content store database.

Cognos Content Database

Cognos Content Database is an instance of an Apache Derby database. It is a selectable component, and is not installed by default. If you install it on the same computer as Content Manager, Cognos Content Database is configured as the default content store for Cognos 8.

Cognos Content Database can be used if you do not want to implement a third-party database for the content store.

Apache Derby is open source software whose license terms can be found on the Apache Derby web site (http://db.apache.org/derby/license.html). Modifying the Apache Derby database or using it with other products is not supported by Cognos. Any modifications that you make to the Apache Derby database are at your own risk.

You can use Cognos Content Database as a content store or notification database, but not as a query database.

Composite Information Server

Composite Information Server provides access to additional data sources such as LDAP, JDBC, Open XML and WSDL, and improves performance when querying data from different data sources.

Cognos 8 Samples

The Cognos 8 samples illustrate product features and technical and business best practices using data from a fictitious company, Great Outdoors. You can also use them for experimenting with and sharing report design techniques, and for troubleshooting.

Modeling Components

Modeling components model data within data sources to structure and present data in a way that is meaningful to users. Modeling components include the following tools:

Framework Manager

Framework Manager is the Cognos 8 modeling tool for creating and managing business-related metadata for use in Cognos 8 analysis and reporting. Metadata is published for use by reporting tools as a package, providing a single, integrated business view of any number of heterogeneous data sources.

Metric Designer

Metric Designer is the Cognos 8 modeling tool used to create extracts for use in Cognos 8 scorecarding applications. Extracts are used to map and transfer information from existing metadata sources such as Framework Manager and Impromptu Query Definition (.iqd) files.

Cognos 8 Transformer

Cognos 8 Transformer is the Cognos 8 modeling tool used to create PowerCubes for use in Cognos 8. Secured Cognos 8 PowerCubes are not compatible with Cognos Series 7.

For information about installing and configuring versions of Transformer that are earlier than 8.3, see the documentation provided with your edition of Transformer.

Series 7 IQD Bridge

The Series 7 IQD Bridge contains the connection information that Cognos 8 requires to use Cognos Series 7 Impromptu IQD data sources and Cognos 8 Framework Manager externalized queries in Cognos 8 Transformer.

Map Manager

Administrators and modelers use a Windows utility named Map Manager to import maps and update labels for maps in Report Studio. For map features such as country and city names, administrators and modelers can define alternative names to provide multilingual versions of text that appears on the map.

For information about using Map Manager, see the Map Manager *Installation and User Guide*.

Third-party Components

In addition to the tools provided with Cognos 8, it requires the following components that are created using third-party resources.

Content Store

The content store is a relational database that contains data that Cognos 8 needs to operate, such as report specifications, published models, and the packages that contain them; connection information for data sources; information about the external namespace, and the Cognos namespace itself; and information about scheduling and bursting reports. The relational database can be Cognos Content Database or a database from a supported third-party vendor.

Design models and log files are not stored in the content store.

The Cognos 8 service that uses the content store is named Content Manager.

Metric Store

A metric store is a relational database that contains content for metric packages. A metric store also contains Metric Studio settings, such as user preferences.

More than one metric store may be created. For example, one metric store may contain content for a sales application and another metric store may contain content for a finance application.

Data Sources

Data sources, also known as query databases, are relational databases, dimensional cubes, files, or other physical data stores that can be accessed through Cognos 8. Application Tier Components use data source connections to access data sources.

Chapter 3: Distribution Options for Cognos 8

Before implementing Cognos 8, decide how you will install it in your environment. You can install all Cognos 8 components on one computer, or distribute them across a network. The best distribution option depends on your reporting or scorecarding requirements, resources, and preferences. Configuration requirements differ depending on whether you install all components on one computer or more than one computer.

Cognos 8 is compatible with other Cognos products. If your environment includes other Cognos products, you must consider how Cognos 8 will fit into that environment.

Distributing Cognos 8 Reporting Components

When you install Cognos 8 reporting components, you specify where to place the gateways, Application Tier Components, and Content Manager. You can install these components using any of these options:

- Install all components on one computer.

  This option is typically used for a demonstration or in a proof of concept environment.

- Install the gateway on a separate computer.

  In this option, the gateway and Web server are on one computer, and the remaining Cognos components are on other computers. You may choose this option if you have existing Web servers available to handle Cognos component requests.

- Install Application Tier Components and Content Manager on separate computers.

  Choose this option to maximize performance, availability, capacity, or security based on the processing characteristics of your organization.

  If you plan to install Cognos Content Database, you can install it on the same computer as Content Manager or on another computer. If you install it on the same computer, Cognos Content Database is automatically configured for use as your content store. If you install it on another computer, ensure that you set the connection properties for Cognos Content Database on your Content Manager computer.

- Install Cognos 8 reporting components on the same computer as other Cognos 8 products.

  Cognos 8 shares components for reporting and for scorecarding, such as the Content Manager. If you plan to install both Cognos 8 reporting and scorecarding components on the same computer, we recommend that you install them in the same installation location.

After installing Cognos 8 reporting components, you must configure them so they can communicate with each other.

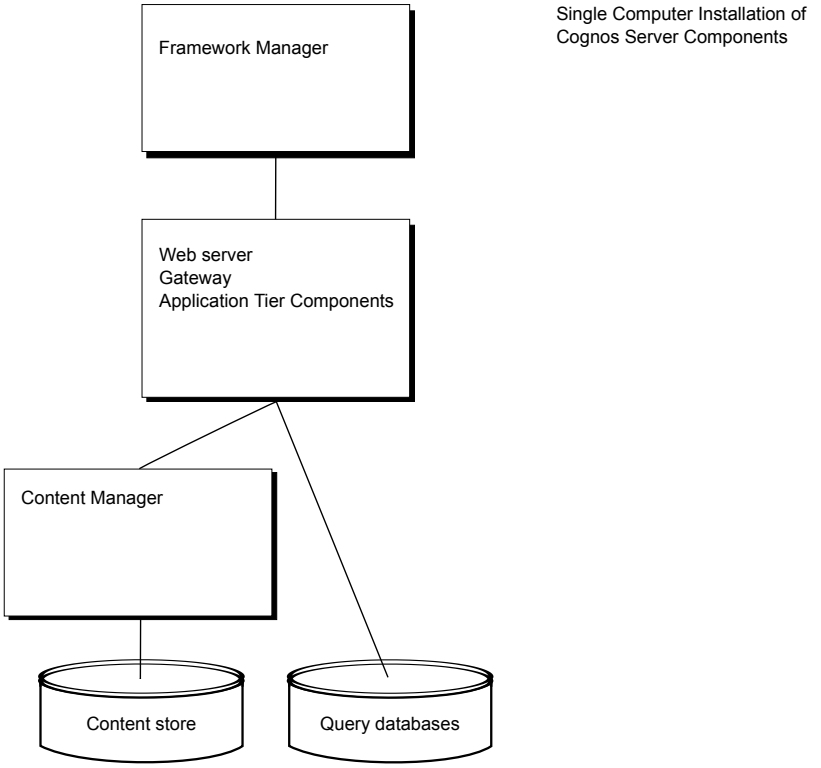
In addition to installing the Content Manager, Application Tier Components, and gateway components, you must install Framework Manager, the metadata modeling application for business intelligence. You can also choose to install Transformer, the modeling and building tool for creating PowerCubes for use with Cognos 8. No matter which Cognos installation scenario you follow, you can install Framework Manager or Transformer, and the content store on a computer separate from the Application Tier Components.

All Components on One Computer

You can install all the Cognos 8 reporting components on one computer. Choose this scenario for proof of concept or demonstration environments where the user load is small.

Because the gateway must be located with the Web server, the single computer must also be running a Web server. If your Web server is on UNIX or Linux, you must install the Windows-based Framework Manager on a separate computer that runs on Windows.

In the following diagram, all server components for Cognos 8 reporting, except Framework Manager, are installed on one computer. The content store, query databases, and Framework Manager are located on separate computers.



Configuration Requirements

If you install all server components for Cognos 8 reporting on the same computer, you must then

- configure your Web server to view Cognos content
- specify connection information to the content store
- set up an email account for notifications (if you intend to email reports)

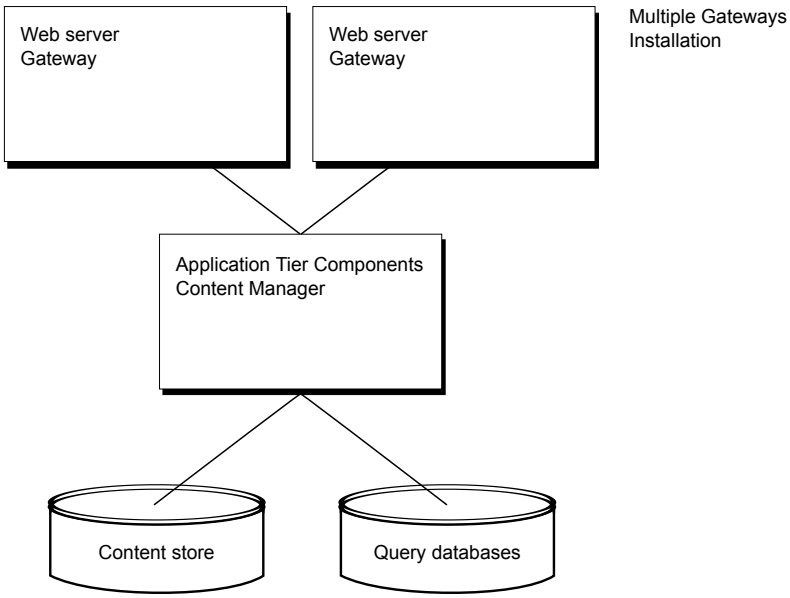
Gateways on Separate Computers

The gateway manages communications among Cognos 8 reporting components. It can reside on one or more Web servers.

You can install the gateway and a Web server on one computer, and install the remaining Cognos 8 reporting components on other computers. If you have a Web farm, you may want to install a gateway on each Web server. Using multiple Web servers to manage incoming requests provides a better level of service.

If you install only the gateway component on the same computer as the Web server, your Web server manages the core Web services and does not process user requests. This separation of processing may be required if you have a firewall between the Web server and your Application Tier Components computers.

In the following diagram, two Web servers each have a gateway installed. Incoming requests are passed to either gateway and forwarded to the Application Tier Components computer.



Configuration Requirements

If you install one or more gateways on separate computers, you must ensure that you can view Cognos content and that the gateways can communicate with other Cognos components. On each computer where the gateway is installed you must

- configure cryptographic properties
- configure your Web server to view Cognos content
- configure the Dispatcher URIs

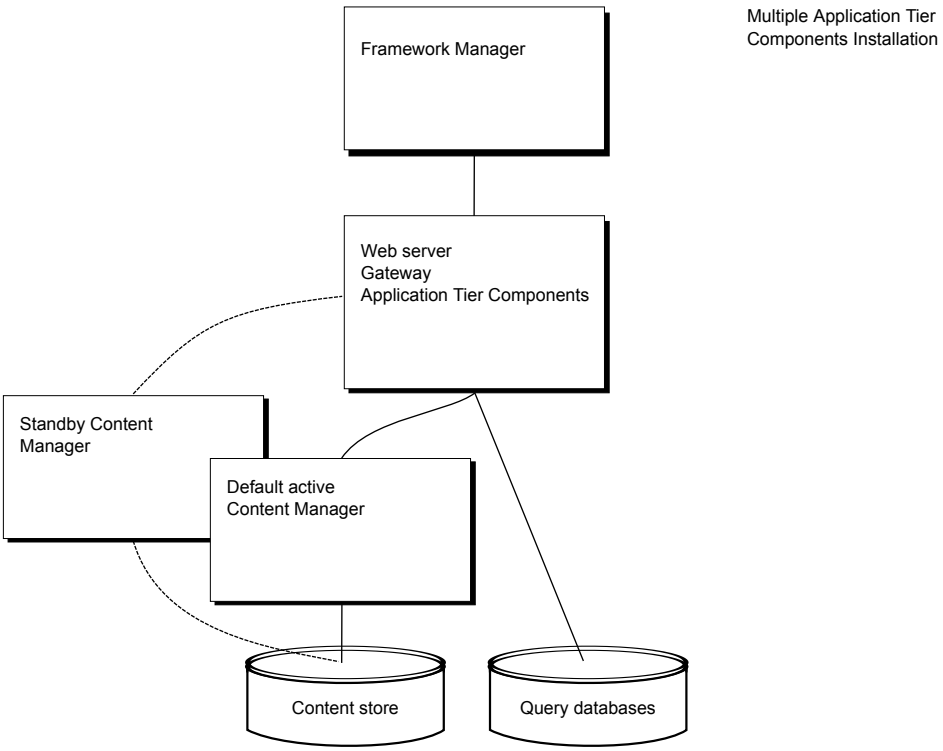
Application Tier Components and Content Managers on Separate Computers

One or more report servers use the Cognos Connection interface to balance loads, access data, perform queries, schedule jobs, and render reports. Content Manager stores all report specifications, results, packages, folders, and jobs in the content store.

You can install the Application Tier Components and Content Manager on the same computer, or on different computers. Installing on different computers can improve performance, availability, and capacity.

To improve scalability in an environment in which there is typically a large volume of report requests to process, you can install the Application Tier Components on multiple computers dedicated to processing incoming requests. By installing the Application Tier Components on multiple computers, you distribute and balance loads among the computers. You also have better accessibility and throughput than on a single computer, as well as failover support.

In the following diagram, incoming requests are routed to a gateway. The gateway forwards the request to one of the Application Tier Components computers. The report server forwards the request to Content Manager, which queries the content store and sends the results back to the report server for rendering.



Configuration Requirements

If you install one or more Application Tier Components on a separate computer, to ensure that they can communicate with other Cognos 8 reporting components you must

- configure cryptographic properties
- specify all Content Manager URIs
- specify the Dispatcher URIs

- specify the Dispatcher URI for external applications

More Than One Content Manager

You can install any number of installations of Content Manager, although only one is active at any time. The other installations each act as a standby Content Manager. One becomes active only if the computer on which the active Content Manager is installed fails. For failover support, it is advisable to install Content Manager on two or more computers.

Content Manager stores data that Cognos 8 needs to operate, such as report specifications, published models, and the packages that contain them; connection information for data sources; information about the external namespace and the Cognos namespace itself; and information about scheduling and bursting reports. The content store is a relational database management system (RDBMS). There is only one content store for each Cognos installation.

You may choose to install Content Manager separately from the Application Tier Components if your data contains sensitive information. Data is then stored in the data tier along with your security information.

When an active Content Manager fails, unsaved session data is lost. When the new active Content Manager takes over, users may be prompted to logon.

Configuration Requirements

On each computer where you install Content Manager, you must

- configure cryptographic properties
- specify connection information to the content store
- specify the Dispatcher URIs
- specify all Content Manager URIs
- specify the Dispatcher URI for external applications
- setup an email account for notifications (if you want to email reports)

Cognos 8 Products on the Same Computer

Cognos 8 products are designed to share components, including the gateway, Content Manager, content store, Cognos Connection, and Cognos Configuration. If you install more than one Cognos 8 product on the same computer, we strongly recommend that you install them in the same installation location. The installation program checks to determine whether other Cognos 8 components exist in the installation location. If a component exists and can be shared, it is not reinstalled.

Accessing Product Documentation in an Integrated Environment

The documentation for Cognos 8 components is installed with the gateway component. If you integrate different Cognos 8 products, you can either use the same gateway or use separate gateways. If you want to use the same gateway, all gateway components must be of the same product version,

and you should install the Cognos 8 gateway component for each product into the same location on the same computer. This ensures that all of the product documentation is available to all users. If you want to use separate gateways for each product, you can install the Cognos 8 gateway component for each product on separate computers, but the product documentation on each gateway will be specific for the Cognos 8 product you installed.

If you want users to access each Cognos 8 product through separate gateways, yet still be able to access documentation for all components, you can install each product's gateway component into the same location as your other Cognos 8 gateway components.

Distributing Framework Manager Components

Framework Manager can be installed on a computer that contains other Cognos 8 reporting components or on a computer that is separate from other Cognos 8 reporting components.

Framework Manager stores run-time models on the Application Tier Components computer. It can communicate with the server using one of two routes:

- connect to the Application Tier Components dispatcher using the Internal dispatcher URI. This route is the recommended route.
- connect to an additional, dedicated gateway that is configured to connect to the dispatcher using the Internal dispatcher URI. You must configure appropriate security for this gateway. This method is useful when the modeling tool is outside a network firewall.

  Note: Do not change your main gateway to use the Internal dispatcher URI. Doing so reduces the security of the Cognos 8 portal and studios.

Where you install Framework Manager, and how you configure it, can depend on how large your metadata models are and on which Web server you use.

Web Servers Other Than Microsoft IIS

For Web servers other than Microsoft Internet Information Services (IIS), no functional difference exists between the two communication routes between the modeling tool and the Application Tier Components dispatcher. For either route, the modeling tool uses the BI Bus SOAP API. If you use the Web server route, and you have medium- and large-sized packages (approaching 1 MB), the models are broken into smaller pieces (chunked) for transmission.

If you use a Web server other than Microsoft IIS, we recommend that you configure the modeling tool to communicate through your Web server gateway (using the first route). This eliminates the need to set up additional communications channels if you use firewalls to separate the modeling tool, Web server, and Application Tier Components.

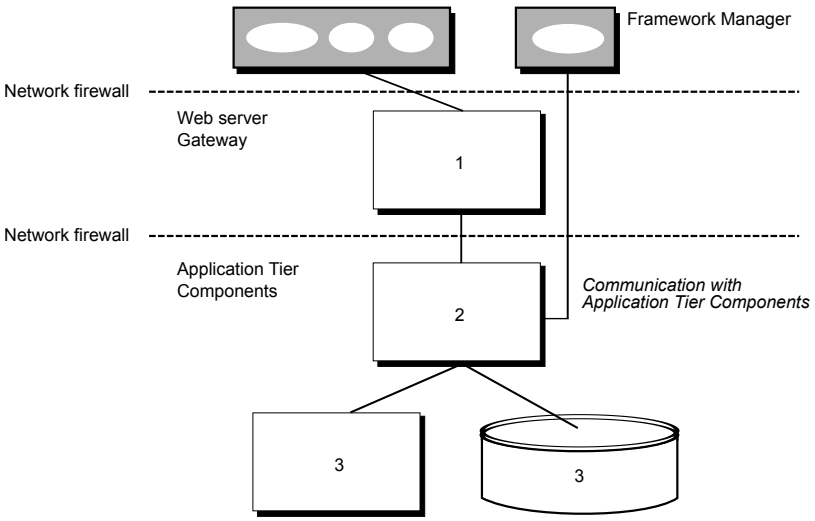
For more information about configuring Framework Manager, see "Configuring Framework Manager Computers" (p. 176).

Firewall Considerations

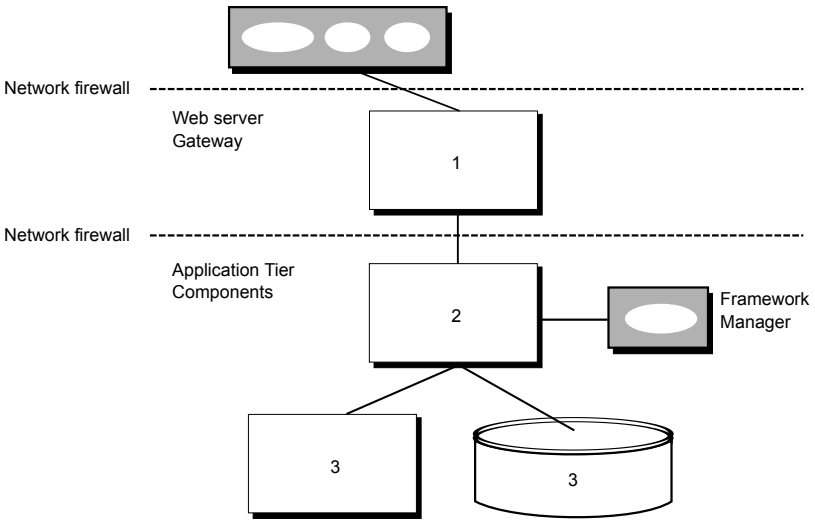
When the modeling tool is outside a network firewall that protects the Application Tier Components, communication issues with the dispatcher can occur. For security reasons, the default Cognos 8

configuration prevents the dispatcher from accepting requests from the modeling tool when it is outside the network firewall.

By default, the modeling tool is configured to send requests directly to the dispatcher:



To avoid communication issues when communicating directly with the dispatcher, install the modeling tool in the same architectural tier as the Application Tier Components.



Alternatively, you can install an additional gateway that is dedicated for communication with the modeling tool. You then configure the modeling tool and its gateway such that the dispatcher will accept requests from the modeling tool.

Configuration Requirements

Framework Manager communicates with the Application Tier Components, which can be installed on one or more Web servers. To publish models, you must configure Framework Manager to communicate with the dispatcher, either directly or through a dedicated gateway.

You must ensure that Framework Manager can communicate with Cognos 8 reporting components. On the computer where Framework Manager is installed, configure cryptographic properties and the following environment properties:

- Gateway URI
- Dispatcher URI for external applications

If the modeling tool is using a dedicated gateway instead of communicating directly with the dispatcher, you must also configure the Dispatcher URIs for gateway property on the dedicated gateway computer.

Distributing Transformer Components

Transformer can be installed on a computer that contains other Cognos 8 components or on a computer that is separate from other Cognos 8 components. When installed separately, Transformer can be used as a standalone product or it can be configured to communicate with other Cognos 8 components.

When you use Transformer as a standalone product, you can use data sources that are external to Cognos 8 and you cannot create secured views with dimensional filtering. When you use Transformer with other Cognos 8 components, you can use the following features provided by Cognos 8:

- Cognos 8 authentication providers
- Cognos 8 data sources, such as published packages, Query Studio reports, and Report Studio reports
- Cognos Connection for publishing the PowerCube datasource and package
- building PowerCubes on Linux or HP-UX Itanium

  You cannot use flat files as data sources.

Transformer consists of the following components. You may have one or both, depending on your environment.

- Transformer Windows

  This is the modeling tool for designing PowerCubes that are used in Cognos 8. It can also be used to build and publish PowerCubes.

- Transformer UNIX/Linux

  This is a command line utility for building PowerCubes. You first design the models using Transformer Windows or MDL scripting, and then use the models to build the PowerCubes.

Either component can communicate with the server using one of two routes:

- connect to the Application Tier Components dispatcher using the internal dispatcher URI (the recommended route).
- connect to an additional, dedicated gateway that is configured to connect to the dispatcher using the internal dispatcher URI. You must configure appropriate security for this gateway. This route is useful when the modeling tool is outside a network firewall.

  Note: Do not change your main gateway to use the internal dispatcher URI. Doing so reduces the security of the Cognos 8 portal and studios.

Web Servers Other Than Microsoft IIS

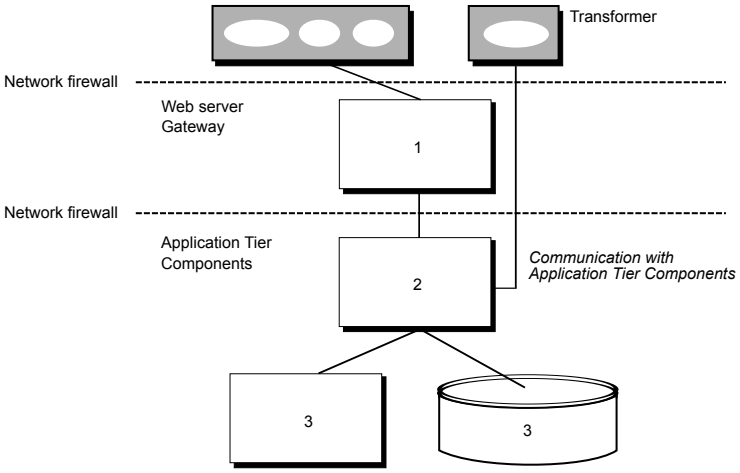
For Web servers other than Microsoft Internet Information Services (IIS), no functional difference exists between the two communication routes between the modeling tool and the Application Tier Components dispatcher. For either route, the modeling tool uses the BI Bus SOAP API. If you use the Web server route, and you have medium- and large-sized packages (approaching 1 MB), the packages are broken into smaller pieces (chunked) for transmission. When publishing packages, only the package run time model is transferred and not the PowerCube. However, the PowerCube must be in a location that the dispatcher can access.

If you use a Web server other than Microsoft IIS, we recommend that you configure the modeling tool to communicate through your Web server gateway (using the first route). This eliminates the need to set up additional communications channels if you use firewalls to separate the modeling tool, Web server, and Application Tier Components.

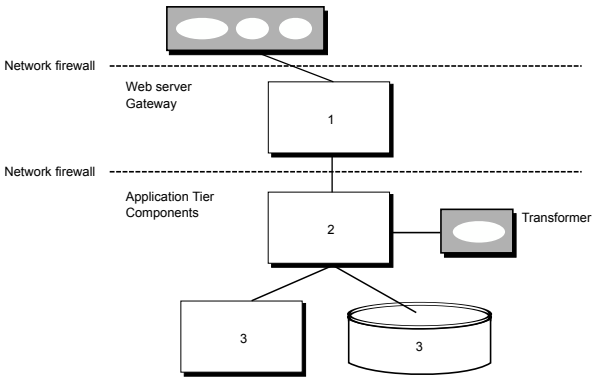
Firewall Considerations

When the modeling tool is outside a network firewall that protects the Application Tier Components, communication issues with the dispatcher can occur. For security reasons, the default Cognos 8 configuration prevents the dispatcher from accepting requests from the modeling tool when it is outside the network firewall.

By default, the modeling tool is configured to send requests directly to the dispatcher:



To avoid communication issues when communicating directly with the dispatcher, install the modeling tool in the same architectural tier as the Application Tier Components.



Alternatively, you can install an additional gateway that is dedicated to communication with the modeling tool. You then configure the modeling tool and its gateway such that the dispatcher accepts requests from the modeling tool.

Role-based Server Considerations

You may want to set up dedicated Transformer servers for optimal cube build performance and accessibility to the Cognos 8 users. In this scenario, consider the following requirements:

- Database client software is installed on any computer that will be used to build or test data in Transformer for PowerCubes.
- Appropriate environment variables are set for UNIX and Linux servers.
- Cognos 8 servers have access to the location where PowerCubes are stored so that the dispatcher can access the PowerCubes.

Building and updating production PowerCubes can be scripted and run remotely when sufficient access and user privileges are set up. For more information about building and updating production PowerCubes, see the Transformer *User Guide*.

Business Analysts or Specialists

You may have specialized business or power users who want to build PowerCubes that are modeled on a combination of corporate and personal data sources. These users may want to do their own analysis of the data for their line of business or a small group of users. You can enable such users to be self-sufficient within the IT and security infrastructure of the organization by meeting the following requirements:

- Database client software is installed, or available for modelers to install, on the Transformer computers that are used to access Cognos 8 data sources or Cognos Series 7 IQD data sources.
- Modelers must have privileges to create a data source in Cognos Administration.

  Modelers do not need direct access to Cognos Administration. They can create and update data sources by using Transformer or command line tools. You can provide modelers with a secured folder in Cognos Connection in which to publish PowerCube packages.
- Modelers must have access to a location in which to store the PowerCube after building it.

  This location must also be accessible to the Cognos 8 service and can be a secured share on a LAN.
- Modelers may require special privileges to remotely run the Cognos 8 PowerCube Connection utility, which is located on the Cognos 8 server. For more information, see the topic about updating published PowerCubes and PowerCube connections in the Transformer *User Guide*.
- To build PowerCubes on a specific Transformer server, modelers should have FTP privileges to transfer models and execute privileges to build cubes on that server.

  Modelers can transfer models and execute cube builds using scripts. Modelers can also use automated methods to build PowerCubes. For more information, see the *Administration and Security Guide*.

Configuration Requirements

To publish PowerCube packages, you must configure Transformer to communicate with the dispatcher, either directly or through a dedicated gateway. If Cognos Connection is secured, you must have privileges to create data sources and publish packages in Cognos Connection.

On the computer where Transformer is installed, configure cryptographic properties and the following environment properties:

- Gateway URI
- Dispatcher URI for external applications

If the modeling tool is using a dedicated gateway instead of communicating directly with the dispatcher, you must also configure the Dispatcher URIs for gateway property on the dedicated gateway computer.

Distributing Cognos 8 Scorecarding Components

When you install Cognos 8 scorecarding components, you specify where to place the gateways, Application Tier Components, and Content Manager. You can install these components using any of these options:

- Install all components on one computer.

  This option is typically used for a demonstration or in a proof of concept environment.

- Install the gateway on a separate computer.

  In this option, the gateway and Web server are on one computer, and the remaining Cognos components are on other computers. You may choose this option if you have existing Web servers available to handle Cognos component requests.

- Install Application Tier Components and Content Manager on separate computers.

  Choose this option to maximize performance, availability, capacity, or security based on the processing characteristics of your organization.

  If you plan to install Cognos Content Database, you can install it on the same computer as Content Manager or on another computer. If you install it on the same computer, Cognos Content Database is automatically configured for use as your content store. If you install it on another computer, ensure that you set the connection properties for Cognos Content Database on your Content Manager computer.

- Install Cognos 8 scorecarding components on the same computer as other Cognos 8 products.

  Cognos 8 products share components, such as Content Manager. If you plan to install Cognos 8 scorecarding components on the same computer as other Cognos 8 products, we recommend that you install them in the same installation location.

After installing Cognos 8 scorecarding components, you must configure them so they can communicate with each other.

In addition to installing the Content Manager, Application Tier Components, and gateway components, you may choose to install Metric Designer (p. 111), the metadata modeling application for scorecarding. No matter which Cognos installation scenario you follow, you can install Metric Designer and the content store on a computer separate from the Application Tier Components.

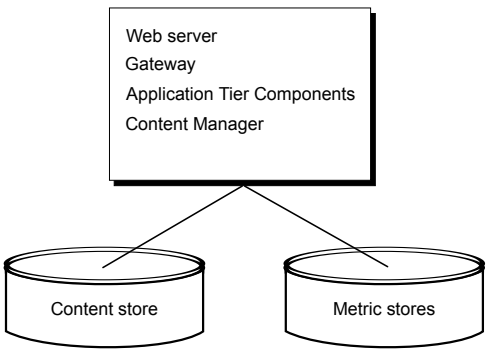
The metric store is usually installed on the same computer as Content Manager. The metric store can also be installed on a different computer.

All Components on One Computer

You can install all the Cognos 8 scorecarding components on one computer. Choose this scenario for proof of concept or demonstration environments where the user load is small.

Because the gateway must be located with the Web server, the single computer must also be running a Web server. If your Web server is on UNIX, you must install the Windows-based Metric Designer on a separate computer that runs on Windows.

In the following diagram, all Cognos 8 scorecarding components, except Metric Designer, are installed on one computer. The content store and metric store are located on separate computers.



Single-Computer Installation of Cognos 8 Scorecarding Components

Configuration Requirements

If you install all Cognos 8 scorecarding components on the same computer, you must

- configure your Web server to view Cognos content
- specify connection information to the content store

Gateways on Separate Computers

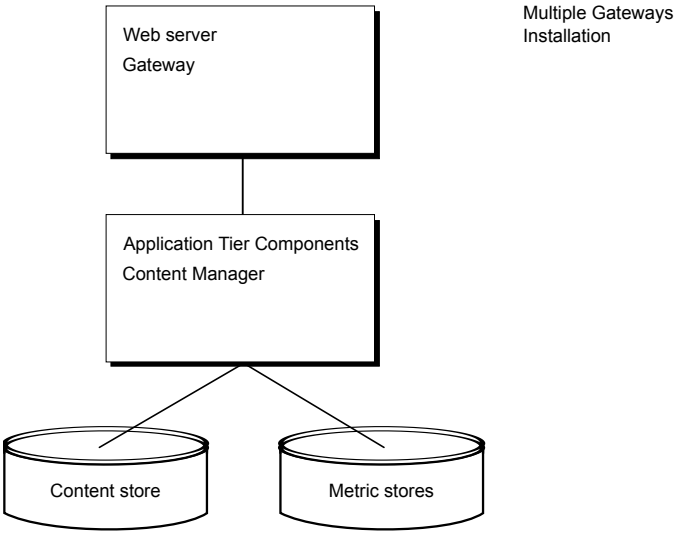
The gateway manages communications among Cognos 8 scorecarding components. It can reside on one or more Web servers.

You can install the gateway and a Web server on one computer, and install the remaining Cognos 8 scorecarding components on other computers. If you have a Web farm, you may want to install a gateway on each Web server. Using multiple Web servers to manage incoming requests provides a better level of service.

If you install only the gateway component on the same computer as the Web server, your Web server manages the core Web services and does not process user requests. This separation of

processing may be required if you have a firewall between the Web server and your other Cognos 8 scorecarding components.

In the following diagram, two Web servers each have a gateway installed. Incoming requests are passed to either gateway and forwarded to the Application Tier Components computer for processing.



Multiple Gateways Installation

Configuration Requirements

If you install one or more gateways on a separate computer, you must ensure that you can view Cognos content and that the gateways can communicate with other Cognos components. On each computer where the gateway is installed, you must

- configure cryptographic properties
- configure your Web server to view Cognos content
- configure the Dispatcher URIs

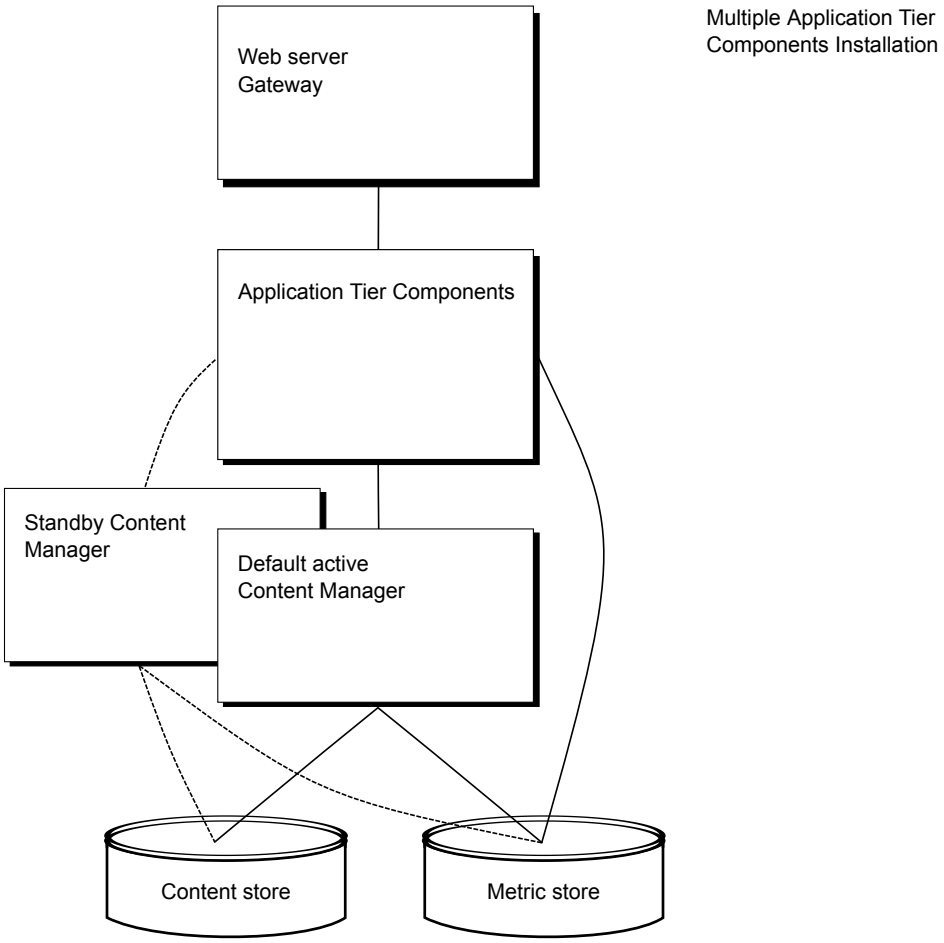
Application Tier Components and Content Managers on Separate Computers

Application Tier Components process Cognos requests, balance loads, execute tasks, and render scorecards. Content Manager stores and retrieves information, such as the data source connections in the content store.

You can install the Application Tier Components and Content Manager on the same computer, or on different computers. Installing on different computers can improve performance, availability, and capacity.

To improve scalability in an environment in which there is typically a large volume of report requests to process, you can install the Application Tier Components on multiple computers dedicated to processing incoming requests. By doing this, you distribute and balance loads among the computers. You also have better accessibility and throughput than on a single computer, as well as failover support.

In the following diagram, incoming requests are routed to a gateway. The gateway forwards the request to one of the Application Tier Components for processing.



Configuration Requirements

If you install one or more Application Tier Components on a separate computer, ensure that they can communicate with other Cognos 8 components. You must

- configure cryptographic properties
- specify all Content Manager URIs
- specify the Dispatcher URIs

More Than One Content Manager

You can install any number of installations of Content Manager, although only one is active at any time. The other installations each act as a standby Content Manager. One becomes active only if the computer on which the active Content Manager is installed fails. For failover support, it is advisable to install Content Manager on two or more computers.

Content Manager stores data that Cognos 8 needs to operate, such as report specifications, published models, and the packages that contain them; connection information for data sources; information about the external namespace and the Cognos namespace itself; and information about scheduling and bursting reports. The content store is a relational database management system (RDBMS). There is only one content store for each Cognos installation.

You may choose to install Content Manager separately from the Application Tier Components if your data contains sensitive information. Data is then stored in the data tier along with your security information.

When an active Content Manager fails, unsaved session data is lost. When the new active Content Manager takes over, users may be prompted to logon.

Configuration Requirements

On each computer where you install Content Manager, you must

- configure cryptographic properties
- specify connection information to the content store
- specify the Dispatcher URIs
- specify all Content Manager URIs

Cognos 8 Products on the Same Computer

Cognos 8 products are designed to share components, including the gateway, Content Manager, content store, Cognos Connection, and Cognos Configuration. If you install more than one Cognos 8 product on the same computer, we strongly recommend that you install them in the same installation location. The installation program checks to determine whether other Cognos 8 components exist in the installation location. If a component exists and can be shared, it is not reinstalled.

Distributing Metric Designer Components

For Metric Studio, if you want to define and load a large amount of metrics from relational and dimensional data sources, including cubes, Framework Manager packages, or Impromptu Query Definitions (.iqd files), install Metric Designer to extract the data.

Install Metric Designer after installing and configuring other Cognos 8 components. If other Cognos 8 components are running in a UNIX environment, you must install the Windows-based Metric Designer on a Windows computer.

If Metric Designer is installed on a different Windows computer from other Cognos 8 components, communication can occur using one of two routes:

- connect to the Application Tier Components dispatcher using the Internal dispatcher URI. This route is the recommended route.
- connect to an additional, dedicated gateway that is configured to connect to the dispatcher using the Internal dispatcher URI. You must configure appropriate security for this gateway. This method is useful when the modeling tool is outside a network firewall.

  Note: Do not change your main gateway to use the Internal dispatcher URI. Doing so reduces the security of the Cognos 8 portal and studios.

Where you install Metric Designer, and how you configure it, can depend on how large your metadata models are and which Web server you use.

Web Servers Other Than Microsoft IIS

For Web servers other than Microsoft Internet Information Services (IIS), no functional difference exists between the two communication routes between the modeling tool and the Application Tier Components dispatcher. For either route, the modeling tool uses the BI Bus SOAP API. If you use the Web server route, and you have medium- and large-sized packages (approaching 1 MB), the models are broken into smaller pieces (chunked) for transmission.

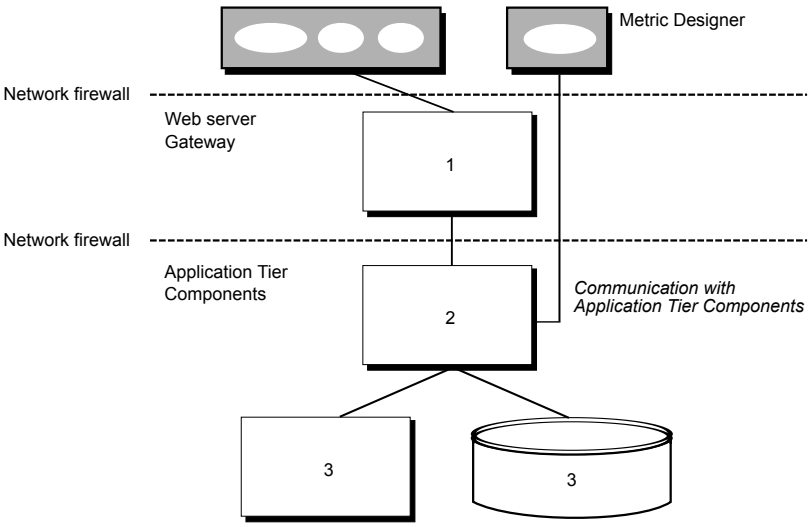
If you use a Web server other than Microsoft IIS, we recommend that you configure the modeling tool to communicate through your Web server gateway (using the first route). This eliminates the need to set up additional communications channels if you use firewalls to separate the modeling tool, Web server, and Application Tier Components.

For more information about configuring Metric Designer, see "Configure Metric Designer" (p. 188).

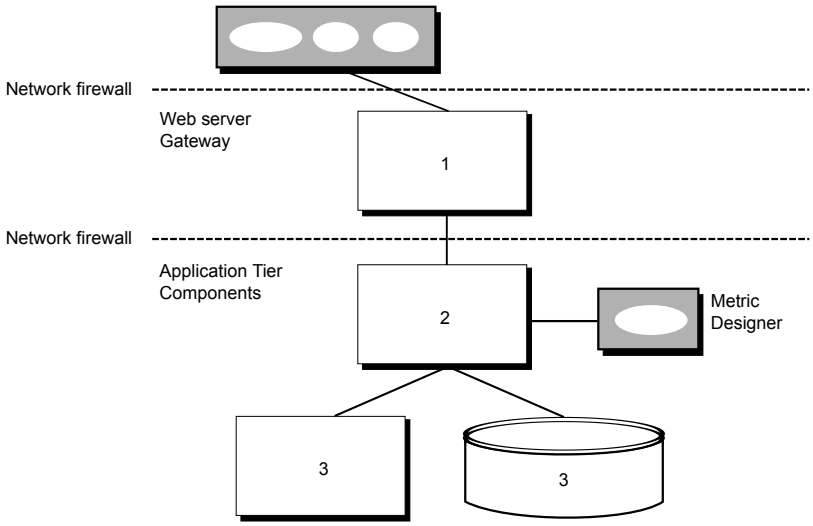
Firewall Considerations

When the modeling tool is outside a network firewall that protects the Application Tier Components, communication issues with the dispatcher can occur. For security reasons, the default Cognos 8 configuration prevents the dispatcher from accepting requests from the modeling tool when it is outside the network firewall.

By default, the modeling tool is configured to send requests directly to the dispatcher:



To avoid communication issues when communicating directly with the dispatcher, install the modeling tool in the same architectural tier as the Application Tier Components.



Alternatively, you can install an additional gateway that is dedicated for communication with the modeling tool. You then configure the modeling tool and its gateway such that the dispatcher will accept requests from the modeling tool.

Configuration Requirements

Metric Designer communicates with the Application Tier Components, which can be installed on one or more Web servers. To publish extracts, you must configure Metric Designer to communicate with the dispatcher, either directly or through a dedicated gateway.

You must ensure that Metric Designer can communicate with other Cognos 8 scorecarding components. On the computer where Metric Designer is installed, configure cryptographic properties and the following environment properties:

- Gateway URI
- Dispatcher URI for external applications

Additional configuration is required after you install Metric Designer so that it can access some types of data sources (p. 188).

If the modeling tool is using a dedicated gateway instead of communicating directly with the dispatcher, you must also configure the Dispatcher URIs for gateway property on the dedicated gateway computer.

Cognos 8 with Other Cognos Products

You can install Cognos 8 in an environment that includes other Cognos products. The installation wizard for Cognos 8 can recognize compatible directories and shows a warning when conflicts occur. After Cognos 8 is installed, you can access objects that are created in another Cognos product in Cognos 8. The requirements for access depend on how you choose to run the two products.

Cognos Products That Can Be Upgraded to Cognos 8

The following Cognos products are earlier versions of components that are now within Cognos 8: ReportNet, Cognos Metrics Manager, DecisionStream, and PowerPlay Web. When you upgrade these products to Cognos 8, you can continue to run the earlier versions concurrently in the same environment until you are satisfied with the transition to Cognos 8.

ReportNet®

For ReportNet and Cognos 8 to run concurrently, each version must have unique ports, content stores, aliases, and cookie settings. If you use the default settings, configuration is required only to select new ports and a new content store for Cognos 8. You cannot use data from ReportNet directly in Cognos 8 until you upgrade ReportNet. When you upgrade to Cognos 8, the content store is upgraded to use the Cognos 8 schema. You can upgrade reports at the same time or upgrade them later if compatibility is required with some existing SDK applications.

Cognos Metrics Manager

To use data store content from Cognos Metrics Manager in Cognos 8, you upgrade by exporting the content from the data store, installing Cognos 8, and then importing the content into the Cognos 8 metric store. Note that the cube picker feature (the ability to map specific metrics to cube intersections) in Cognos Metrics Manager is not available in Cognos 8.

Cognos DecisionStream

You can continue to run Cognos DecisionStream Series 7 concurrently with Cognos 8 products. Catalogs that are created using DecisionStream Series 7 must be upgraded before you can use them with Data Manager.

For instructions about running concurrently and upgrading DecisionStream catalogs to the Cognos 8 Data Manager environment, see the chapter about upgrading a catalog in the Data Manager *User Guide*.

Cognos PowerPlay Web

You can continue to use PowerPlay Web reports within the PowerPlay 7 user interfaces in the Cognos 8 portal. You can also drill through between PowerPlay Web and Cognos 8. You can publish from PowerPlay Enterprise Server to Cognos 8, provided that you use the same host name or IP address to identify the Series 7 namespace in Cognos Series 7 and in Cognos 8.

You can also upgrade the following reports to Cognos 8 reports by using migration tools:

- PowerPlay Windows reports
- PowerPlay Web Explorer reports
- PowerPlay for Excel reports
- PowerPlay for Windows reports published to PowerPlay Web

The tools are available at the Cognos Global Customer Services Web site (support.cognos.com).

For instructions about upgrading, see the Migration Tools *User Guide*.

Cognos Series 7 Products That Can Be Migrated to Cognos 8

You can migrate metadata and applications from Cognos Series 7 to Cognos 8. Content that can be migrated includes Architect models from Windows, Impromptu client reports and catalogs from Windows, Upfront content, and Web-based content from Windows and UNIX.

For more information, see the Migration Tools *User Guide*.

For a list of supported Cognos Series 7 versions and to download the migration tools and documentation, see the Cognos Global Customer Services Web site (http://support.cognos.com).

Architect

You can migrate Architect models for use as a metadata source for Framework Manager.

Impromptu

You can migrate Impromptu catalogs and reports to Cognos 8. You use migrated catalogs as a metadata source for Framework Manager. After completing the catalog migration process, you can migrate and deploy Impromptu reports.

Upfront

You can migrate Upfront content to Cognos 8. The migration process maps the Upfront content structure to a Cognos Connection folder structure. By preserving the existing Upfront organization, it is easier to complete administrative tasks, such as applying security to the migrated content.

Impromptu Web Reports

You can migrate Impromptu Web Reports content, such as schedules and events, to Cognos 8. You migrate Impromptu Web Reports content using a Cognos Series 7 Deployment Manager package as the migration source. Before you migrate Impromptu Web Reports you must migrate the Impromptu catalog metadata used by the reports.

You cannot migrate Impromptu query definition files (.iqd), but you can continue to use existing .iqd files to build cubes in Cognos 8 BI Transformer 8.3. To do so, you must install the optional component, Series 7 IQD Bridge, which is available to install with Cognos 8 BI on Cognos Series 7 supported platforms.

PowerPrompts are not migrated, but you can implement similar functionality using either the built-in administrator functionality or the Software Development Kit.

Cognos Products That Interoperate with Cognos 8

Some Cognos products provide functionality that is not available in Cognos 8. You can use these products in the same environment as Cognos 8. With some products, you can access the different types of cubes or reports in the Cognos 8 portal. With other products, you can access unique features in the Cognos 8 portal.

Cognos Planning - Analyst

You can access published plan data in Cognos 8 by using the Generate Framework Manager Model wizard, which requires Cognos Planning - Analyst 7.3 MR1 or later.

For more information, see the Analyst *User Guide*.

Cognos Planning - Contributor

You can access unpublished (real-time) Contributor cubes in Cognos 8 by custom installing the Cognos 8 - Contributor Data Server component that is included with Cognos Planning - Contributor 7.3 MR1 release or later. You can access published plan data in Cognos 8 by using the Generate Framework Manager Model administration extension in Contributor, which requires Cognos Planning - Contributor 7.3 MR1 or later.

For more information, see the Contributor *Administration Guide*.

Cognos Finance

You can access Cognos Finance cubes that are secured against a Series 7 namespace by using the Cognos Finance Network API Service. You can also export data and metadata from Cognos Finance for use in Framework Manager.

Cognos Controller

You can access Cognos 8 to create Cognos Controller Standard Reports by using a predefined Framework Manager model that is created when Cognos Controller is installed. You can also access published Controller data and structures in Framework Manager for custom reporting and analysis. Both Cognos Controller and Cognos 8 BI must be at the same version.

Transformer

You can use Cognos PowerCubes and Transformer models that were generated by Transformer 7.3 or later directly in Cognos 8. The cubes and models are upwards compatible and require no migration or upgrade tools. You can run reports and analyses in Cognos 8 against the Cognos PowerCubes.

If you want to use the new integration features of Transformer with Cognos 8, you can upgrade Cognos Series 7.x Transformer models to Cognos 8 BI Transformer 8.3. This allows you to use Cognos 8 data sources (such as published packages), list reports authored in Query Studio or Report Studio, authenticate using Cognos 8 security, and publish directly to Cognos Connection.

Before you load the model, the Cognos Series 7 namespace must be configured in Cognos 8 (p. 263) and the name ID that is used to configure it in Cognos 8 must match the name used in Cognos Series 7.

For more information about upgrading Cognos Series 7 secured PowerCubes, see the Cognos 8 Transformer *User Guide*.

For Cognos Series 7 PowerCubes to be used in Cognos 8, we recommend that you optimize the cubes for use in Cognos 8 by using the pcoptimizer utility, which is supplied with Cognos 8. Otherwise, PowerCubes that were created with previous versions of Transformer may take too long to open in the Cognos 8 Web studios. This optimization utility is suitable for older PowerCubes

when the model no longer exists or the data used to build the PowerCube is no longer available. It is not necessary to run this command line utility for cubes created in Transformer 8.3. For more information about optimizing PowerCubes, see the Transformer *User Guide*.

You can publish PowerCubes using Transformer 8.3, Framework Manager, or directly in the Cognos 8 portal. You can publish single PowerCube data sources and packages to Cognos Connection interactively in Transformer or in the command line. You can also publish silently using batch scripts after building a PowerCube. A user who has privileges to create data sources and packages in Cognos Connection can publish PowerCubes in Cognos Connection as well. The MDC file must be in a secured location that the Cognos 8 dispatcher can access. Packages that use multiple PowerCubes or PowerCubes mixed with other data sources should be published using Framework Manager.

If you use a Cognos Series 7 PowerCube as a data source, Cognos 8 converts the cube data from the encoding that was used on the system where the PowerCube was created. For a successful conversion, Cognos Series 7 PowerCubes must be created with a system locale set to match the data in the PowerCube.

Data Manager

Data Manager is used to create data warehouses and data repositories for reporting, analysis, and performance management. When Data Manager is installed in your Cognos 8 environment, you can use the Data Movement Service to run builds and JobStreams in Cognos Connection. You must install the Data Manager engine in the same location as your Cognos 8 Application Tier Components. Both Data Manager and Cognos 8 BI must be the same version.

Cognos 8 Go! Mobile

With Cognos 8 Go! Mobile you can access reports authored with Analysis Studio, Report Studio, and Query Studio on a mobile device (such as a BlackBerry®). To download, view, and interact with reports, Cognos 8 Go! Mobile requires the installation of a custom-built, rich client on the mobile device, in addition to the Cognos 8 server components. Both Cognos 8 Go! Mobile and Cognos 8 BI must be at the same version.

Cognos 8 Go! Search

The Cognos 8 Go! Search add-on provides enhanced search and navigation options in Cognos 8. In Cognos Connection, you can use full-text search to locate content. In Analysis Studio, Query Studio, and Cognos Viewer, you can use full-text search and automatic navigation, which locates content related to the content in the current view. The Cognos 8 content store must include content that can be indexed. Both Cognos 8 Go! Search and Cognos 8 BI must be at the same version.

Cognos Series 7 Content That Can Be Recreated in Cognos 8

Some Cognos products cannot be programmatically migrated or upgraded with the migration or upgrade tools for Cognos 8. Cognos 8 offers two options for duplicating content or functionality for the products described below: use the Upfront portal in the Cognos 8 portal or duplicate queries, visualizations, or objects by using Cognos 8 studios.

Cognos Query

You can use the migration tools to identify Cognos Query objects in the Cognos Series 7 migration source. You can then duplicate most Cognos Query functionality in Cognos 8. Foundation queries are available in Cognos 8 when you migrate an Architect model. You can also manually replicate saved queries using SQL components in Report Studio.

Cognos Visualizer

You can duplicate functionality by using the charting, layout, and formatting options in Report Studio and Analysis Studio.

Cognos NoticeCast

You can duplicate alert and notification functionality by using Event Studio and other Cognos 8 components.

Cognos Web Services

You can duplicate most Cognos Web Services functionality using the Cognos 8 Software Development Kit.

CognosScript

You can duplicate automation functionality using the Cognos 8 Software Development Kit.

Cognos Portal Services

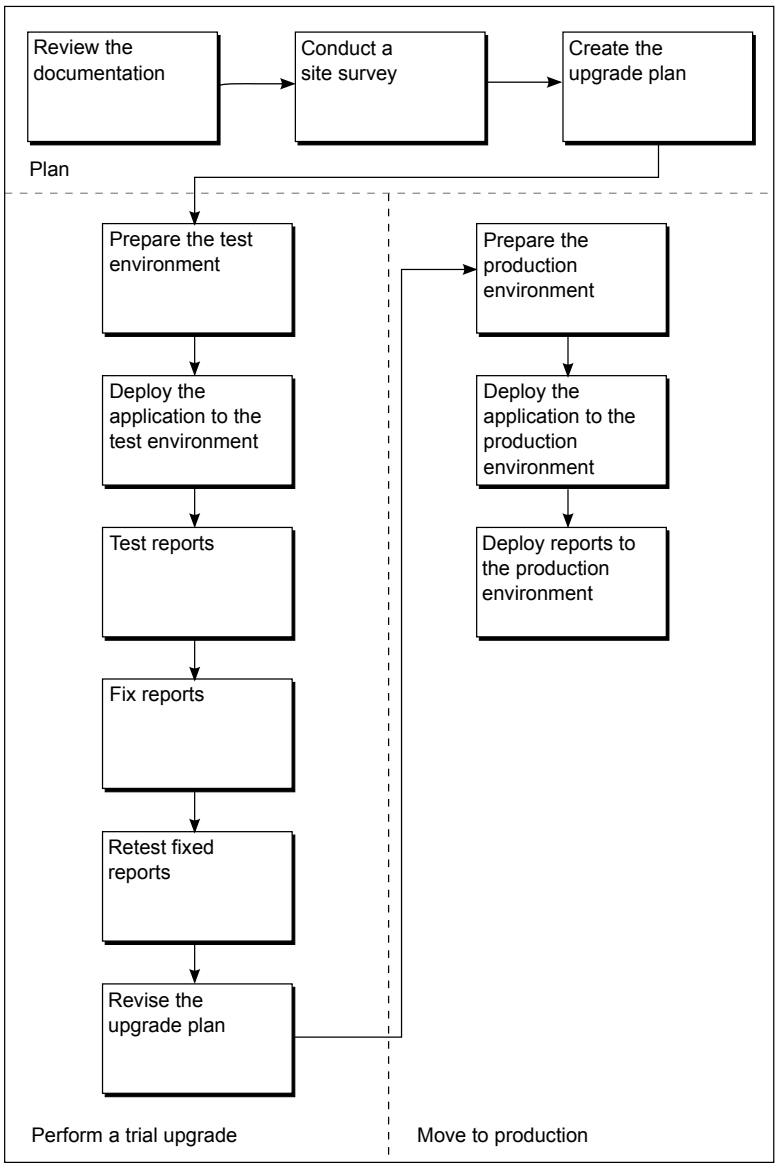
You can duplicate most Cognos Portal Services functionality using Cognos Connection.

Chapter 4: Upgrading to Cognos 8

If you have Cognos Series 7 content, you can move some of that content to Cognos 8 using migration tools that are available in a separate installation.

If you are using previous versions of ReportNet, Metrics Manager, Cognos 8 Go! Office, or Transformer, you can upgrade your content to Cognos 8. You can also upgrade from previous versions of Cognos 8, including full and maintenance (MR) releases.

Upgrading Cognos 8 is a process that you perform in stages. The following workflow shows the tasks that are performed at each stage of the process in a typical upgrade.



In the preparation stage, gather information, assess your reporting environment, and develop the upgrade plan. In the trial upgrade stage, upgrade your Cognos 8 applications and reports in a test

environment. In the move to production stage, apply what you learned in the test environment to deploy your configuration from the test environment to the production environment.

In some upgrade situations, other tasks may be required. For example, if you use SDK applications that depend on the report specifications, you must upgrade your SDK applications before upgrading the report specifications.

See the following topics for information about upgrading:

- Planning the Upgrade
- Upgrading from Cognos Series 7
- Upgrading from ReportNet, Metrics Manager, or Earlier Versions of Cognos 8
- Upgrading Cognos 8 Go! Office
- Upgrading Transformer Models and PowerCubes

Planning the Upgrade

We recommend that you plan your upgrade so that you know what to expect at each stage of the process. In the planning stage, you can review the upgrade documentation for information about expected behavior, new features, deprecated features, compatibility between versions, and requirements for preparing your production environment. When you finish the review, you can then conduct a site survey to identify the BI infrastructure, applications, reports, and custom configuration settings. Finally, you can test the upgrade on a subset of your data so that you can fine tune your reports and data before committing to the full upgrade.

Use the following checklist to guide you through the planning process:

- Review the documentation
- Conduct a site survey
- Perform a trial upgrade
- Review the move to the production environment

Review the Documentation

Cognos provides documentation from a variety of sources to help you achieve a successful upgrade. All of the documentation is available online at the Cognos Global Customer Services Web site (http://support.cognos.com).

Steps

1. Read the "What's New" section in this guide (p. 15).

   It contains a list of new, changed, deprecated, and removed features for this release.

2. Read the rest of the Upgrade information in this document.

3. Read the topic about Cognos 8 with other Cognos products (p. 43).

It contains information about other Cognos products that you may have in your environment and that must be considered in the upgrade.

4. From the Documentation link on the Cognos Global Customer Services Web site (http://support.cognos.com), download and review the latest versions of the following documentation:
   - Cognos 8 *Readme*

     The Readme is regularly updated to document issues that might affect you during an upgrade.
   - the document *Upgrading to Cognos 8 BI 8.3: Changes in Product Behavior* (http://support.cognos.com/go/docs/cognos8_bi/8.3/changes_productbehavior.html)

     This document includes examples of the changed behavior and solutions for issues that may occur during the upgrade.
   - Cognos 8 *New Features Guide*
   - the "What's New" and upgrade sections of the Framework Manager *User Guide*
   - the "What's New" and upgrade sections of the Report Studio Professional Authoring *User Guide*
   - the "What's New" and upgrade sections of the Cognos 8 Transformer *User Guide*

     Read these sections only if you use Transformer.
   - Cognos 8 Migration Tools *User Guide*

     This document describes how to upgrade metadata, Impromptu catalogs and reports, PowerPlay reports, and Upfront content from Cognos Series 7 to Cognos 8.
   - the release notes and upgrade sections of the Cognos 8 SDK *Developer Guide*

     Read these sections only if you use SDK applications.
   - all Best Practices documents about upgrading

Conduct a Site Survey

Do a site survey to assess the current production environment and identify areas that require attention during an upgrade. The site survey should include information about the infrastructure, applications, users, and configuration settings for your Cognos 8 products.

Steps

1. Assess the third-party software that you use in your reporting application by doing the following:
   - List third-party software, such as operating systems, Web servers, security, databases, and so on.
   - Compare the list to the supported versions for your target upgrade version, available from the Production Information, Software Environments links at the Cognos Global Customer Services Web site (http://support.cognos.com).

- Determine whether any third-party components require updating.

2. List your BI applications, including
   - Framework Manager models, packages, and reports
   - Metrics Manager packages, projects, and extracts
   - SDK applications and their dependencies
3. List content that you plan to migrate or upgrade from other Cognos products, such as Transformer models and PowerCubes.
4. List all the reports contained in your application and do the following:
   - Flag heavily used reports and high-profile reports for priority treatment during the upgrade.

     Use audit report data to determine report usage. For more information about audit reports, see the *Administration and Security Guide*.
   - Flag reports that fail to run or validate in the current environment.

     They are unlikely to upgrade successfully. Repair these reports so that they upgrade.
   - Consider retiring unused or little-used reports.
5. If you will be upgrading Transformer models, list the models that you want to upgrade.
6. List the following information about your configuration:
   - configuration settings that you enabled using Cognos Configuration

     These settings are preserved through the upgrade. They are stored in two files. For ReportNet, the files are crnstartup.xml and crnlocale.xml. For Cognos 8, the files are cogstartup.xml and coglocale.xml.
   - changes to other configuration files

     Changes to other files must be made manually during the upgrade. If you changed other configuration files, you must assess the changes that you want to preserve in the upgraded environment. This may include .xml, .txt, and .css files in the configuration, templates, webapps, and webcontent directories of the installation location.

     Important: Changes to .ini files are not supported. If you changed .ini files, please contact Customer Support.
7. Back up all reports, models, and configuration data and files
8. Create an upgrade plan.

Perform a Trial Upgrade

We recommend that you perform a trial upgrade several weeks before upgrading your production system. The trial upgrade identifies components that will upgrade with minimal effort and components that may require additional actions before or after the upgrade.

Steps

1. Prepare the test environment:
   - Install the new release system in the test environment.
   - Configure the test system to match your production environment.
   - Manually configure customization.
2. Deploy your current reporting application on the test system:
   - Upgrade report specifications from the source to the test system.
   - Validate report specifications on the test system.
3. Test your reports:
   - In Report Studio, validate each report and note whether the validation was successful.
   - In Report Studio, Query Studio, and Analysis Studio, run the applicable reports and note whether each report ran successfully.
4. Test models and PowerCubes in Cognos 8 Transformer, if required:
   - Open models with the appropriate security options and save them.
   - Test PowerCubes.
5. Repair or exclude reports and models that do not operate correctly.
6. Test the repaired reports and models by running them again on the test system.

   Troubleshoot any issues, and contact Cognos Support about unresolved upgrade issues.
7. Revise the upgrade plan to include adaptations that you made during the trial upgrade.

Review the Move to the Production Environment

When all issues that you discovered during the trial upgrade are resolved, you are ready to begin the full upgrade in your production environment. Your upgrade plan will provide the details for each step of the full upgrade.

The steps below are a summary of the process. For detailed steps, see "Upgrading from ReportNet, Metrics Manager, or Earlier Versions of Cognos 8" (p. 55).

Steps

1. Prepare the production environment:

- Back up files and data.
- Install your new release system in the production environment.
- Configure the system.
- Manually configure customization.

2. Deploy the application on the production system.
3. Deploy the reports and models from the test system to the production system.

Upgrading from Cognos Series 7

You can move content from Cognos Series 7 to Cognos 8. For a list of supported versions, see the Cognos Global Customer Services Web site (http://support.cognos.com). If you are using a version of Cognos Series 7 that is not supported for migrating to Cognos 8, you must first upgrade the software and data to a supported version of Cognos Series 7. Moving other Cognos Series 7 content to Cognos 8 is considered a migration.

You can move the following types of content to Cognos 8:

- Cognos Series 7 Web-based content, such as PowerPlay Web Explorer reports, from Windows and UNIX
- PowerPlay Windows reports
- Upfront content, such as NewsBoxes and NewsIndexes, from Windows and UNIX
- Impromptu reports and catalogs from Windows
- Impromptu Web Reports content, such as events, schedules, and Impromptu reports and catalogs that are published in Impromptu Web Reports as reports
- Architect models from Windows
- Transformer PowerCubes, including user class views and user classes from models with secured cubes

If you have published PowerPlay Web reports to Cognos Connection, either the ReportNet version or the Cognos 8 version, you can continue to open the PowerPlay Web reports in PowerPlay Web Explorer or you can upgrade the PowerPlay Web reports to Cognos 8 Analysis.

Transformer allows you to place security objects from different namespaces within a single custom view. Cognos 8 supports multiple namespaces for securing PowerCubes, but only to verify content when migrating from Cognos Series 7 security to an alternate security provider. You cannot deploy PowerCubes that are secured against multiple namespaces in Cognos 8. After verifying the content in the model, you must associate a single namespace with each PowerCube. For more information, see the Transformer *User Guide*. For information about upgrading Series 7 content to Cognos 8 Transformer, see "Upgrading Transformer Models and PowerCubes" (p. 83).

If you are moving content from Cognos Series 7, you must install the Cognos migration tools to upgrade your Cognos Series 7 content to Cognos 8.

You can download the migration tools or you can request a CD. For more information, go to the Cognos Global Customer Services Web site (http://support.cognos.com). The documentation for installing and using the tools is included with the tools.

To upgrade PowerPlay reports that are published to Cognos Connection, after you install the migration tools, you must enable the options to allow users to open the Cognos Series 7 reports in Report Studio or Analysis Studio. You use Cognos Connection to enable the options. For more information, see the *Administration and Security Guide*.

Upgrading from ReportNet, Metrics Manager, or Earlier Versions of Cognos 8

You must upgrade the software to move from an earlier version of Cognos 8, ReportNet, or Metrics Manager to a new version of Cognos 8. You must upgrade all components. Components from different versions are not compatible. If you are using Cognos Series 7 PowerCubes as a data source, it is not necessary to upgrade Transformer unless you want to use the features of the new version of Transformer. For more information, see "Upgrading Transformer Models and PowerCubes" (p. 83). PowerCubes that are built using Series 7.3 Transformer (or later) and Cognos 8.3 Transformer are both supported with Cognos 8 reporting and metrics.

You can upgrade directly to Cognos 8 from the following product versions:

- Cognos 8 8.1 or later, including MR releases
- ReportNet 1.1 MR1 through MR4
- Metrics Manager 2.0 or later

If you have an earlier version of ReportNet, you must first upgrade to one of the ReportNet 1.1 MR releases (1 through 4) and then upgrade to Cognos 8.

You can run different versions of the software on your computer at the same time, provided that you install them in different directories and configure each to use a different content store and a different set of ports and URLs for each version.

Before you begin upgrading, you must plan your upgrade strategy (p. 50). The strategy depends on the data that you want to use and any customizing that you have done with your existing configuration.

When upgrading from ReportNet, if you want to use an existing configuration directory, you must ensure that the configuration data from ReportNet is copied to the Cognos 8 installation location. This includes backing up existing data, configuring Cognos 8 to use the existing content store or a copy of it, copying the configuration data files to the Cognos 8 installation directory, and reapplying any manual edits or customizations that you applied in the earlier version.

If both ReportNet and Metrics Manager are on the same computer and you plan to upgrade to Cognos 8, upgrade ReportNet first, and then Metrics Manager.

After upgrading to Cognos 8 using existing data, additional configuration may be required if you want to use new features. For information about new features in Cognos 8, see Cognos 8 *New Features*.

SDK Applications

You must use the Cognos 8 SDK with Cognos 8 Business Intelligence.

When you upgrade, you must make some changes to your SDK program for it to function with the Cognos 8 version of the WSDL file. Some methods, classes, and properties have been deprecated in Cognos 8. Deprecated features continue to function as before, but will be removed in future releases. Some other methods, classes, and properties are obsolete, and have been removed from the Cognos 8 SDK.

For information about changes to methods, classes, properties, and enumeration sets, see the Release Notes appendixes in the Cognos 8 SDK *Developer Guide*.

New report specifications have been added in Cognos 8. If you run a ReportNet report in Cognos 8, it is automatically upgraded to the Cognos 8 format. After a report is upgraded to Cognos 8, it cannot be returned to the ReportNet format. Because of the potential for users to upgrade report specifications that SDK applications may depend on, we recommend that you set access permissions on those reports to limit user access. For more information about setting access permissions, see the Cognos 8 *Administration and Security Guide*.

Do not upgrade your report specifications if you have SDK applications that create, modify, or save report specifications. You must first update your SDK applications to comply with the Cognos 8 report specifications schema. Otherwise, your SDK applications may not be able to access the upgraded report specifications. For information about upgrading report specifications, see the Cognos 8 SDK *Developer Guide*.

We recommend that you do not upgrade your report specifications if you are unsure about whether you have SDK applications that create, modify, or save report specifications. Contact your SDK administrator for more information about your SDK applications.

Content Manager

When you upgrade ReportNet, Content Manager automatically upgrades the schema and contents in the content store. After you upgrade, you cannot use the upgraded content store with ReportNet because it is not backward compatible. To protect your original content store data, you must configure Cognos 8 to use a copy of the content store. You create a copy by backing up the original content store and restoring the data into a new content store.

Cognos 8 can read deployment archives produced by ReportNet.

Content Store

If you saved reports from Series 7 PowerPlay or scorecards from Cognos Metrics Manager 2.x in ReportNet, the content store upgrade carries the saved reports and scorecards forward into Cognos 8.

Framework Manager

You can use the same models and projects in Framework Manager for Cognos 8 that you used with the earlier version. When upgrading models, the validation process produces errors for every model. To upgrade a project, you open and save it in the new version of Framework Manager. For more information, see the Framework Manager *User Guide*.

If you have SDK applications that rely on an earlier version of the report specifications, you cannot use Framework Manager to publish your model without losing backward compatibility.

Report Studio

The upgrade does not account for such items as undocumented and unsupported features, changes in report behavior, and changes in formatting and style sheets. For more information, see the Report Studio Professional Authoring *User Guide*.

Published Series 7 PowerCubes in ReportNet

If you published cubes from Cognos Series 7 PowerPlay Enterprise Server in ReportNet, you may not be able to publish those same cubes in Cognos 8. The default cookie path that was used in ReportNet is changed in Cognos 8. To enable publishing of your Cognos Series 7 PowerCubes in Cognos 8, see "Set Up to Publish Series 7 PowerCubes After Upgrade from ReportNet" (p. 80).

Metrics Manager Data Stores

In earlier versions, Metrics Manager used a data store database to store, organize, and retrieve information. In Cognos 8, this database is referred to as the metric store. If you want to use data store content from an earlier version, you can export the content from the data store, install Cognos 8, and import the content into the metric store.

You cannot use the metric store with the earlier version of Metrics Manager because it is not backward compatible. Before exporting the data store content, ensure that you back it up, in case you must revert to the earlier version.

Metric Designer

You can upgrade projects from earlier versions of Metrics Manager if you want to use them with Cognos 8 Metric Designer (p. 190).

You cannot use upgraded projects with the earlier version because they are not backward compatible. Before upgrading projects, ensure that you have backed them up, in case you need to revert to the earlier version.

Security

When you upgrade from ReportNet or an earlier version of Cognos 8, security may be affected. For example, new roles may exist that were not in earlier releases and some roles may have new capabilities. As a result, the security of your upgraded system may not be at the desired level. To confirm the security level after upgrading, see the *Administration and Security Guide*.

Operating Systems

As you upgrade your Cognos 8 products, you may choose to install some components on new operating systems. You must consider how these operating systems might affect the installation and configuration of Cognos 8.

If your upgrade includes installing Cognos 8 components on Windows Vista, you must consider the following:

- roaming profiles

  Profiles of users are stored in a different location than in earlier Windows operating systems. The Documents and Settings directory is replaced by the Users directory. The All Users directory is replaced by the Public directory.

- environment variables

  The default paths that are associated with environment variables are changed. If you use scripts or applications that reference the paths in the environment variables, you may need to update the scripts and applications.

  In addition, you must reconfigure the default file locations in Cognos Configuration so that a single file location can be used across operating systems in your Cognos 8 environment. For more information, see the topics about updating file location properties in the configuration chapter (p. 165).

Installations That Include Earlier Versions of Other Cognos 8 Products

In you are upgrading Cognos 8 BI in an environment that includes earlier versions of other Cognos 8 products, such as Cognos 8 Controller 8.2, Cognos 8 Planning 8.2, or Cognos 8 BI Analysis for Excel 8.2, install the new version of Cognos 8 BI in a separate location from the other Cognos 8 product and configure Cognos 8 BI to operate independently of that product. After you upgrade the other product to a compatible version with Cognos 8 BI, you can then configure the two products to operate together.

Upgrade from an Earlier Version of Cognos 8

You can upgrade Cognos 8 in the same directory as an earlier version or in a different directory.

If you want to upgrade Cognos 8 in the same directory, you must first back up your data, ensure that Framework Manager projects are not checked into a source control system, and uninstall the older version of Cognos 8. For complete instructions, see the steps to install in the same directory.

If you are installing on a new computer, see the steps to install in a new directory.

When you back up the configuration data, you store it in a secure directory. The directory must be protected from unauthorized or inappropriate access.

An alternative method of upgrading is to export the entire content store to a deployment archive and then import the deployment archive into Cognos 8 after the upgrade. For more information about deployment, see the *Administration and Security Guide*. A deployment upgrade is required if you want to change the type of database that you use for the content store. If you use the

deployment upgrade method, only the steps for exporting and restoring the configuration data are different. All other steps are the same as documented in this section.

Cognos 8 installs and uses Tomcat as its application server by default. If you do not want to use Tomcat, you must follow a different set of steps to upgrade. For more information, see "Upgrade to Cognos 8 in an Application Server Environment " (p. 311).

When you upgrade, the report administrator will no longer have access to the Content Administration tool. The report administrator will not be able to create deployment definitions in Cognos 8.

Customized Cognos 8 Files

If you manually edited any configuration files, the changes will be overwritten during the upgrade. You must reapply the changes. You should keep a record of any customizations to ensure that they can be reapplied after upgrading. You should also back up these files so that the original version can be restored if necessary.

You may have modified files other than those in the configuration folder. If so, you should also back up the additional files before upgrading.

The Cognos 8 presentation service supports automatic upgrade of some system.xml files. If you made many customization changes to system.xml files, you can use this automatic upgrade feature instead of reapplying the changes manually after upgrading. The system.xml files are overwritten during the installation of Cognos 8. Therefore, you must back up the customized versions of these files and then copy them to the directory after upgrading Cognos 8. The automatic upgrade will be applied when you start the Cognos 8 service.

The system.xml files for which automatic upgrade is supported are in the following directories:

- *c8_location*/templates/ps
- *c8_location*/templates/ps/portal
- *c8_location*/templates/ps/qs

Note: The recommended method to upgrade customized files is to manually reapply changes after the new software is installed. Automatic upgrade of system.xml files is to be used only when you have made a large number of customizations to these files.

Steps to Install in the Same Directory

1. Using your database tools, back up your existing content store database.

   For information on how to do this, see the documentation for your database.

2. Back up the following files to a secure location:
   - coglocale.xml in the *c8_location*/configuration directory
   - server.xml in the *c8_location*/tomcat4.1.27/conf directory
   - system.xml in the appropriate directory, if required

   Ensure that you note the directory path. For example,

   c8_location/templates/ps

3. In Cognos Configuration, export the configuration data to the same secure location.

   To make the data usable for upgrading, name the file cogstartup.xml.

   Important: Because the exported crnstartup.xml file contains unencrypted passwords, ensure that the location is secure.

4. Back up any manually edited files in the *c8_location*/configuration and other directories to a secure location.

5. Stop all Cognos services.

6. If you use a source control system such as CVS, ensure that all Framework Manager projects you want upgraded are checked out before upgrading.

   Any projects that are checked in when you uninstall will not be upgraded.

7. Prepare Transformer models, if required (p. 83).

8. Upgrade or install third-party products (p. 77).

9. Uninstall Cognos 8 from every Cognos 8 computer (p. 113).

10. Install the newer version of Cognos 8 in the same directory that you used for Cognos 8 on every computer (p. 98).

11. Copy the .xml files from the secure backup location as follows:

    - Copy cogstartup.xml and coglocale.xml to *c8_location*/configuration.
    - Copy server.xml to *c8_location*/tomcat4.1.27/conf.
    - Copy system.xml to the appropriate directory, if required.

      For example,

      c8_location/templates/ps

    If you are prompted to overwrite existing files, click **Yes**.

12. For files that you manually edited in earlier versions of Cognos 8, edit the same files in the *c8_location* directory and reapply the changes that you made to the original customized files.

    Do not copy the customized files to the *c8_location* directories. The earlier versions of these files may not be compatible.

13. If you use Oracle for a data source, import source, logging database, or the content store database, delete the classes12.jar file from the *c8_location*\webapps\p2pd\WEB-INF\lib directory.

    Older versions of Cognos 8 used this file, which conflicts with the ojdbc14.jar file that is used in newer versions.

14. In Cognos Configuration, review the configuration, and then save it.

    When you save the configuration, an upgrade dialog appears and asks if you want to upgrade your report specifications. The default setting is to not upgrade report specifications.

    Important: Do not upgrade your report specifications if you have SDK applications that create, modify, or save report specifications. You must first update your SDK applications to comply

with the Cognos 8 report specifications schema. Otherwise, your SDK applications may not be able to access the upgraded report specifications. In addition, do not save your reports until the SDK applications have been updated. For information about upgrading report specifications, see the Cognos 8 SDK *Developer Guide*.

15. Start Cognos 8.

    Cognos 8 automatically upgrades the content store. System.xml files are upgraded, if required, to a Cognos 8 compatible version.

16. Install (p. 105) and configure (p. 176) Framework Manager.

17. Upgrade your Framework Manager projects and reports (p. 179) as required. For instructions, see the Framework Manager *User Guide*.

    Report Studio users must clear their Web browser cache to get the latest images.

18. If you use pages created in earlier versions of Cognos 8, you may need to reconfigure the following properties:

    - Title
    - Open action links going outside a portal

    For more information, see the *Administration and Security Guide*.

19. Install (p. 108) and configure (p. 181) Transformer, if required.

20. Upgrade Transformer models and PowerCubes (p. 83), if required.

21. If you use SAP Enterprise Portal, upgrade your master iView.

    Old SAP iViews will not work with the new Portal Services producer component. For information, see the topic about deploying Cognos Portlets to SAP Enterprise Portal in the *Administration and Security Guide*.

Steps to Install in a New Directory

1. Using your database tools, copy your existing content store database into a new content store database.

   For information on how to do this, see the documentation for your database.

2. Back up the following files to a secure location:

   - coglocale.xml in the *c8_location*/configuration directory
   - server.xml in the *c8_location*/tomcat4.1.27/conf directory
   - system.xml in the appropriate directory, if required

     Ensure that you note the directory path. For example,

     c8_location/templates/ps
   - In Cognos Configuration, export the configuration data to the same secure location.

     To make the data usable for upgrading, name the file cogstartup.xml.

Important: Because the exported cogstartup.xml file contains unencrypted passwords, ensure that the location is secure.

- Back up any manually edited files in the *c8_location*/configuration and other directories to a secure location.

3. Prepare Transformer models, if required (p. 83).
4. Upgrade or install third-party products (p. 77).
5. Install Cognos 8 in a new directory (p. 93).
6. Copy the .xml files from the secure backup location to the following directory:
   - Copy cogstartup.xml and coglocale.xml to *c8_location*/configuration.
   - Copy server.xml to *c8_location*/tomcat4.1.27/conf.
   - Copy system.xml to the same directory in the new location as it was in the earlier version, if required.

     For example,

     c8_location/templates/ps

   If you are prompted to overwrite existing files, click **Yes**.
7. For files that you manually edited, edit the same files in the *c8_location* directory and reapply the changes that you made to the original customized files.

   Do not copy the customized files to the *c8_location* directories. The earlier versions of these files may not be compatible with Cognos 8.
8. Configure new Web server aliases (p. 132).
9. In Cognos Configuration, configure Cognos 8 to point to the new content store, configure new ports and URLs, use a different cookie path, and then save the configuration (p. 77).

   Ensure that the port numbers and service name for this installation are different from those used for earlier versions so that there are no conflicts.

   Ensure that security authentication settings are not changed. For example, the namespaces must be the same for policies, users, roles, and groups to work correctly.

   When you save the configuration, an upgrade dialog appears and asks if you want to upgrade your report specifications. The default setting is to not upgrade report specifications.

   Important: Do not upgrade your report specifications if you have SDK applications that create, modify, or save report specifications. You must first update your SDK applications to comply with the Cognos 8 report specifications schema. Otherwise, your SDK applications may not be able to access the upgraded report specifications. In addition, do not save your reports until the SDK applications have been updated. For information about upgrading report specifications, see the Cognos 8 SDK *Developer Guide*.
10. Start Cognos 8.

Cognos 8 automatically upgrades the new content store. System.xml files are upgraded, if required, to a Cognos 8 compatible version.

11. Install (p. 105) and configure (p. 176) Framework Manager.
12. Upgrade your Framework Manager projects and reports (p. 179) as required. For instructions, see the Framework Manager *User Guide*.

    Report Studio users must clear their Web browser cache to get the latest images.
13. Open the Administration portal, and unregister the dispatchers that are used with earlier versions of Cognos 8.

    When you open the Administration portal in Cognos 8, you may see the dispatchers that are registered for both versions.

    For more information, see the *Administration and Security Guide*.
14. If you use pages created in ReportNet, you may need to reconfigure the following properties:
    - Title
    - Open action links going outside a portal

    For more information, see the *Administration and Security Guide*.
15. Install (p. 108) and configure (p. 181) Transformer, if required.
16. Upgrade Transformer models and PowerCubes (p. 83), if required.
17. If you use SAP Enterprise Portal, upgrade your master iView.

    Old SAP iViews will not work with the new Portal Services producer component. For information, see the topic about deploying Cognos Portlets to SAP Enterprise Portal in the *Administration and Security Guide*.
18. When you are ready to uninstall the previous version of Cognos 8, do the following:
    - Stop the Cognos 8 service.
    - Uninstall Cognos 8 from all computers.

      For instructions, see "Uninstalling Cognos 8" (p. 113).

When you complete the upgrade tasks, Cognos 8 is fully configured except for new properties and features, and scorecarding features.

If you use Chinese, Japanese, or Korean characters, you may notice differences in some characters after upgrading. For more information, see the Troubleshooting section of the *Administration and Security Guide*.

If you use a DB2 database for the content store, you can tune the database to take advantage of DB2 features. For more information, see the *Architecture and Deployment Guide*.

To ensure the security and integrity of Cognos 8, it is important to protect the installation directory from unauthorized or inappropriate access.

Migrate Apache Derby Databases to Cognos Content Database

If you use your own installation of Apache Derby for the content store or notification databases, you must migrate the databases to Cognos Content Database before starting Cognos 8. To do this, remove the CognosCMDerby.jar file from the Apache Derby database and copy the database directories to the content store directory of the Cognos 8 installation.

Steps

1. Ensure that your Apache Derby Network Server is running.
2. Start the ij utility using the ij.bat or ij.ksh script file.
3. Connect to the Apache Derby database by typing the following ij utility command:

   connect 'jdbc:derby://*host*:*port*/*db_name*;user=*username*;password=*password*';

   Here is an example:

   connect 'jdbc:derby://localhost:1527/cm;user=cognos; password=cognos';

   If you changed the port number from the default 1527, use the correct port number for your Apache Derby database. Use the correct name of your Apache Derby database.
4. Clear the derby.database.classpath property of the database by typing the following ij utility command:

   CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.database.classpath','');
5. Remove the existing jar file by typing the following ij utility command:

   CALL sqlj.remove_jar('*schema_name*.CMFunctionsjar', 0);

   For example, if your schema is cognos, type

   CALL sqlj.remove_jar('cognos.CMFunctionsjar', 0);
6. Enable row level locking on the database by typing the following ij utility command:

   CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.storage.rowLocking','true');
7. Close the ij utility by typing the following command:

   disconnect;
8. Stop the Apache Derby Network Server.
9. Copy the content store and notification database directories to the *c8_location*\contentstore directory.

   For example:

   xcopy "c:\derby\data\cm" "c:\Program Files\c8\contentstore\cm" /s /ixcopy "c:\derby\data\notify_db" "c:\Program Files\c8\contentstore\notify_db" /s /i

   In this example, the content store database is named cm and the notification database is named notify_db. They are located in the c:\derby\data directory.

New Product, File, and Directory Names After Upgrade from ReportNet

After you upgrade from ReportNet, the product name will be changed to Cognos 8. In addition, some file, directory, and command names will be different. If you install Cognos 8 in a different directory from ReportNet, default directory names change when you install Cognos 8. If you install Cognos 8 in the same directory as ReportNet, the existing directory names do not change. Some file name changes occur when you install Cognos 8 and other changes occur after you save the Cognos 8 configuration. You must change the alias for the virtual directory manually, if required.

The following names are affected.

ReportNet name	Cognos 8 name	Description
crn	c8	Default installation directory
crn	cognos8	Default Web browser alias or virtual directory
crnstartup.xml	cogstartup.xml	Configuration data file used when starting Cognos Configuration
crnstartup_ yyyymmddhhmm.xml	cogstartup_ yyyymmddhhmm.xml	Configuration data file that stores choices made each time the configuration is saved
crnlocale.xml	coglocale.xml	Configuration data file that stores codes for global configuration settings
crnlocale_ yyyymmddhhmm.xml	coglocale_ yyyymmddhhmm.xml	Configuration data file that stores choices made each time global configuration settings are saved
crnformat.xml	cogformat.xml	Configuration data file that stores formats for numeric data, dates, and times
crnserver.log	cogserver.log	Default logging file
crconfigw.exe	cogconfigw.exe	File to start Cognos Configuration on Windows
crconfig.bat	cogconfig.bat	File to start Cognos Configuration in silent mode on Windows
crconfig.sh	cogconfig.sh	File to start Cognos Configuration on UNIX and Linux

ReportNet name	Cognos 8 name	Description
crconfig.prefs	cogconfig.prefs	Configuration data file that stores user preferences for Cognos Configuration
crconfig_ response.csv	cogconfig_ response.csv	Silent mode log file that stores activities performed while Cognos Configuration runs in silent mode
xstartup	issetup	Command to start the installation wizard on XWindows
xwsetup	issetupcc	Command to start the installation wizard on UNIX and Linux
xwsetup.exe	issetup.exe	File to start the installation wizard on Windows
ReportNetService_ languagecode.xml	CognosService_ languagecode.xml	Sample file for medium or large configuration

Upgrade ReportNet to Cognos 8

You can install and upgrade to Cognos 8 in the same directory as ReportNet or in a different directory.

If you want to upgrade Cognos 8 in the same directory, you must first back up your data, ensure that Framework Manager projects are not checked into a source control system, and uninstall ReportNet. For complete instructions, see the steps to install in the same directory.

If you want to install Cognos 8 in a new directory, you can keep ReportNet active until you are satisfied with the operation of the new version. If you are installing on a new computer, see the steps to install in a new directory.

When you back up the configuration data, you store it in a secure directory. The directory must be protected from unauthorized or inappropriate access.

An alternative method of upgrading is to export the entire content store to a deployment archive in ReportNet and then import the deployment archive into Cognos 8. For more information about deployment, see the *Administration and Security Guide*. A deployment upgrade is required if you want to change the type of database that you use for the content store. If you use the deployment upgrade method, only the steps for exporting and restoring the configuration data are different. All other steps are the same as documented in this section.

Cognos 8 installs and uses Tomcat as its application server by default. If you upgrade from ReportNet and you do not want to use Tomcat, you must follow a different set of steps to upgrade. For more information, see "Upgrade to Cognos 8 in an Application Server Environment " (p. 311).

When you upgrade from ReportNet 1.1 to Cognos 8, the report administrator will no longer have access to the Content Administration tool. The report administrator will not be able to create deployment definitions in Cognos 8.

Customized ReportNet Files

If you manually edited any configuration files, the changes will be overwritten during the upgrade. You must reapply the changes in the Cognos 8 environment. You should keep a record of any customizations to ensure that they can be reapplied after upgrading. You should also back up these files so that the original version can be restored if necessary.

You may have modified files other than those in the configuration folder. If so, you should also back up the additional files before upgrading.

The Cognos 8 presentation service supports automatic upgrade of some ReportNet system.xml files. If you made many customization changes to system.xml files in ReportNet, you can use this automatic upgrade feature instead of reapplying the changes manually after upgrading. The system.xml files are overwritten during the installation of Cognos 8. Therefore, you must back up the ReportNet versions of these files and then copy them to the directory after installing Cognos 8. The automatic upgrade will be applied when you start the Cognos 8 service.

The system.xml files for which automatic upgrade is supported are in the following directories:

- *crn_location*/templates/ps
- *crn_location*/templates/ps/portal
- *crn_location*/templates/ps/qs

Note: The recommended method to upgrade customized files is to manually reapply changes after the new software is installed. Automatic upgrade of system.xml files is to be used only when you have made a large number of customizations to these files.

Steps to Install in the Same Directory

1. Using your database tools, back up your existing content store database.

   For information on how to do this, see the documentation for your database.

2. Back up the following files to a secure location:
   - crnlocale.xml in the *crn_location*/configuration directory
   - server.xml in the *crn_location*/tomcat4.1.27/conf directory
   - system.xml in the appropriate directory, if required

   Ensure that you note the directory path. For example,

   crn_location/templates/ps

3. In Cognos Configuration, export the configuration data to the same secure location.

   To make the data usable for upgrading, name the file crnstartup.xml.

   Important: Because the exported crnstartup.xml file contains unencrypted passwords, ensure that the location is secure.

4. Back up any manually edited files in the *crn_location*/configuration and other directories to a secure location.
5. Stop all Cognos services.
6. If you use a source control system such as CVS, ensure that all Framework Manager projects you want upgraded are checked out before uninstalling ReportNet.

   Any projects that are checked in when you uninstall will not be upgraded.
7. Prepare Transformer models, if required (p. 83).
8. Upgrade or install third-party products (p. 77).
9. Uninstall ReportNet from every ReportNet computer.

   For instructions, see the documentation for the older version of ReportNet.
10. Install Cognos 8 in the same directory that you used for ReportNet on every computer (p. 98).
11. Copy the .xml files from the secure backup location as follows:
    - Copy crnstartup.xml and crnlocale.xml to *crn_location*/configuration.
    - Copy server.xml to *crn_location*/tomcat4.1.27/conf.
    - Copy system.xml to the appropriate directory, if required.

      For example,

      crn_location/templates/ps

    If you are prompted to overwrite existing files, click **Yes**.
12. For files that you manually edited in ReportNet, edit the same files in the *crn_location* directory and reapply the changes that you made to the original customized files.

    Do not copy the customized files to the *crn_location* directories. The earlier versions of these files may not be compatible with Cognos 8.
13. If you use Oracle for a data source, import source, logging database, or the content store database, delete the classes12.jar file from the *c8_location*\webapps\p2pd\WEB-INF\lib directory.

    Older versions of Cognos 8 used this file, which conflicts with the ojdbc14.jar file that is used in newer versions.
14. In Cognos Configuration, review the configuration, and then save it.

    When you save the configuration, an upgrade dialog appears and asks if you want to upgrade your report specifications. The default setting is to not upgrade report specifications.

    Important: Do not upgrade your report specifications if you have SDK applications that create, modify, or save report specifications. You must first update your SDK applications to comply with the Cognos 8 report specifications schema. Otherwise, your SDK applications may not be able to access the upgraded report specifications. In addition, do not save your reports until the SDK applications have been updated. For information about upgrading report specifications, see the Cognos 8 SDK *Developer Guide*.

15. Start Cognos 8.

    Cognos 8 automatically upgrades the content store. System.xml files are upgraded, if required, to a Cognos 8 compatible version.

    If the ReportNet service continues to run, manually uninstall the ReportNet service (p. 79).

16. Install (p. 105) and configure (p. 176) Framework Manager.

17. Upgrade your Framework Manager projects and reports (p. 179) as required. For instructions, see the Framework Manager *User Guide*.

    Report Studio users must clear their Web browser cache to get the latest images.

18. If you use pages created in ReportNet, you may need to reconfigure the following properties:

    - Title
    - Open action links going outside a portal

    For more information, see the *Administration and Security Guide*.

19. If you published Cognos Series 7 PowerCubes in ReportNet, restructure your virtual directories or change your cookie path (p. 80).

20. Install (p. 108) and configure (p. 181) Transformer, if required.

21. Upgrade Transformer models and PowerCubes (p. 83), if required.

22. If you use SAP Enterprise Portal, upgrade your master iView.

    Old SAP iViews will not work with the new Portal Services producer component. For information, see the topic about deploying Cognos Portlets to SAP Enterprise Portal in the *Administration and Security Guide*.

Steps to Install in a New Directory

1. Using your database tools, copy your existing content store database into a new content store database.

   For information on how to do this, see the documentation for your database.

2. Back up the following files to a secure location:

   - crnlocale.xml in the *crn_location*/configuration directory
   - server.xml in the *crn_location*/tomcat4.1.27/conf directory
   - system.xml in the appropriate directory, if required

     Ensure that you note the directory path. For example,

     crn_location/templates/ps
   - In Cognos Configuration, export the configuration data to the same secure location.

     To make the data usable for upgrading, name the file crnstartup.xml.

Important: Because the exported crnstartup.xml file contains unencrypted passwords, ensure that the location is secure.

- Back up any manually edited files in the *crn_location*/configuration and other directories to a secure location.

3. Prepare Transformer models, if required (p. 83).
4. Upgrade or install third-party products (p. 77).
5. Install Cognos 8 in a new directory (p. 93).
6. Copy the .xml files from the secure backup location to the following directory:
   - Copy crnstartup.xml and crnlocale.xml to *c8_location*/configuration.
   - Copy server.xml to *c8_location*/tomcat4.1.27/conf.
   - Copy system.xml to the same directory in the new location as it was in the ReportNet location, if required.

     For example,

     c8_location/templates/ps

   If you are prompted to overwrite existing files, click **Yes**.
7. For files that you manually edited in ReportNet, edit the same files in the *c8_location* directory and reapply the changes that you made to the original customized files.

   Do not copy the customized files to the *c8_location* directories. The earlier versions of these files may not be compatible with Cognos 8.
8. Configure new Web server aliases (p. 132).
9. In Cognos Configuration, do the following:
   - For the new Cognos 8 instance, configure Cognos 8 to point to the new content store, configure new ports and URLs, and then save the configuration (p. 77).
   - For ReportNet, configure ReportNet to use a new default cookie path (p. 79).

   Ensure that the port numbers and service name for this installation are different from those used for earlier versions so that there are no conflicts.

   Ensure that security authentication settings are not changed. For example, the namespaces must be the same for policies, users, roles, and groups to work correctly.

   When you save the configuration, an upgrade dialog appears and asks if you want to upgrade your report specifications. The default setting is to not upgrade report specifications.

   Important: Do not upgrade your report specifications if you have SDK applications that create, modify, or save report specifications. You must first update your SDK applications to comply with the Cognos 8 report specifications schema. Otherwise, your SDK applications may not be able to access the upgraded report specifications. In addition, do not save your reports until the SDK applications have been updated. For information about upgrading report specifications, see the Cognos 8 SDK *Developer Guide*.

10. Start Cognos 8.

    Cognos 8 automatically upgrades the new content store. System.xml files are upgraded, if required, to a Cognos 8 compatible version.

11. Install (p. 105) and configure (p. 176) Framework Manager.

12. Upgrade your Framework Manager projects and reports (p. 179) as required. For instructions, see the Framework Manager *User Guide*.

    Report Studio users must clear their Web browser cache to get the latest images.

13. Open the Administration portal in Cognos 8, and unregister the dispatchers that are used with ReportNet.

    When you open the Administration portal in Cognos 8, the portal shows the dispatchers that are registered for both versions.

    For more information, see the *Administration and Security Guide*.

14. If you use pages created in ReportNet, you may need to reconfigure the following properties:

    - Title
    - Open action links going outside a portal

    For more information, see the *Administration and Security Guide*.

15. If you published Cognos Series 7 PowerCubes in ReportNet, restructure your virtual directories or change your cookie path (p. 80).

16. Install (p. 108) and configure (p. 181) Transformer, if required.

17. Upgrade Transformer models and PowerCubes (p. 83), if required.

18. If you use SAP Enterprise Portal, upgrade your master iView.

    Old SAP iViews will not work with the new Portal Services producer component. For information, see the topic about deploying Cognos Portlets to SAP Enterprise Portal in the *Administration and Security Guide*.

19. When you are ready to uninstall ReportNet, do the following:

    - Stop ReportNet.
    - Uninstall ReportNet from all ReportNet computers.

      For instructions, see the documentation for the older version of ReportNet.

When you complete the upgrade tasks, Cognos 8 is fully configured except for new properties and features, and scorecarding features.

If you use Chinese, Japanese, or Korean characters, you may notice differences in some characters after upgrading to Cognos 8. For more information, see the Troubleshooting section of the *Administration and Security Guide*.

If you use a DB2 database for the content store, you can tune the database to take advantage of DB2 features. For more information, see the *Architecture and Deployment Guide*.

To ensure the security and integrity of Cognos 8, it is important to protect the installation directory from unauthorized or inappropriate access.

Upgrading Using the Silent Configuration Option

You can run a silent configuration to upgrade the configuration from ReportNet to Cognos 8. Before you run the silent configuration, you must ensure that the option to upgrade the report specifications is set correctly. If you installed Cognos 8 in a new directory, you must also change the settings for ports and the Web server alias.

If you want to upgrade the configuration in silent mode, follow the steps in the preceding section and stop at the step to configure Cognos 8:

- In the steps to install in the same directory, stop at step 12.
- In the steps to install in a new directory, stop at step 8.

When you reach that step, do not start Cognos Configuration. Instead, perform the following steps and then return to the steps in the preceding section.

- Edit the crnstartup.xml file in *crn_location*/configuration or *c8_location*/configuration and look for the following lines:

```
<crn:parameter
name="doReportSpecUpgrade">
  <crn:value xsi:type="xsd:boolean">false</crn:value>
</crn:parameter>
```

- Set the value for the report specification upgrade:
  - To skip the upgrade of the report specifications, leave the value as false.
  - To upgrade the report specifications, change the value to true.
- Modify other settings as required.

  If you installed Cognos 8 in a new directory, see "Run ReportNet and Cognos 8 at the Same Time" (p. 77) for the settings to modify.
- Type the configuration command:
  - On UNIX or Linux, type

    ./cogconfig.sh -s
  - On Windows, type

    cogconfig.bat -s

Upgrade Metrics Manager to Cognos 8

You must install and upgrade to Cognos 8 in a different directory from the earlier version of Metrics Manager. You can keep Metrics Manager active until you are satisfied with the operation of Cognos 8.

If both ReportNet and Metrics Manager are on the same computer and you plan to upgrade to Cognos 8, upgrade ReportNet first, and then Metrics Manager.

Cognos 8 and earlier versions of Metrics Manager use different security models. If you want to upgrade the security information for the earlier version of Metrics Manager, you must follow a different set of steps to upgrade. For more information, see "Upgrade Metrics Manager and Security Information" (p. 73).

Cognos 8 installs and uses Tomcat as its application server by default. If you upgrade from Metrics Manager and you do not want to use Tomcat, you must follow a different procedure to upgrade. For more information, see "Upgrade from Metrics Manager to Cognos 8 in an Application Server Environment" (p. 312).

Steps

1. Export the contents of any data store that you want to use with Cognos 8 from the earlier version of Metrics Manager.

   For more information, see the documentation provided with your earlier version of Metrics Manager.

2. Install Cognos 8:

   - If you are upgrading only Metrics Manager, install Cognos 8 in a different directory from the earlier version of Metrics Manager (p. 93).
   - If ReportNet is on the same computer as Metrics Manager, follow the steps to upgrade ReportNet to Cognos 8 (p. 66).

3. Set up the environment (p. 117).

   If you exported the contents of one or more data stores in step 1, create one metric store database (p. 118) for the contents of each data store. For each metric store, set up the database client (p. 127) and environment variables on UNIX (p. 130).

4. Create a metric package (p. 154).

5. If you exported content from data stores in step 1, import the contents of each data store into a different metric store.

   For information about importing data, see the Metric Studio *User Guide for Authors*.

6. Install (p. 111) and configure (p. 188) Metric Designer on Windows.

7. Upgrade Metric Designer projects and extracts (p. 190) as required.

8. When you are ready, stop the earlier version of Metrics Manager and uninstall it as described in the documentation provided with it.

To ensure the security and integrity of Cognos 8, protect the installation directory from unauthorized or inappropriate access.

Upgrade Metrics Manager and Security Information

Cognos 8 and earlier versions of Metrics Manager use different security models. Before upgrading to Cognos 8, review the information about Cognos 8 security to determine if it meets your requirements. For information, see the *Administration and Security Guide*.

If the Cognos 8 security model does not meet your requirements and you must upgrade your existing security information, an upgrade utility is available. You use this utility during the upgrade process to map the security permissions for scorecards and metrics in the earlier version to corresponding permissions in Cognos 8.

The upgrade utility does not map the Deny permission if it was used in the earlier version of Metrics Manager. For example, assume a user belongs to two user classes. For the same scorecard, one user class has Read permission and the other user class has Deny permission. After the upgrade utility is run, the user will have only Read permission for the scorecard.

The upgrade utility maps security information for one data store using the information in a control file that you create. This file is a text file. If you plan to upgrade the content of more than one data store, you must create a control file for each data store and run the upgrade utility for each control file.

The following table describes the properties that must be defined in the control file. An example of a control file is provided below the table.

Property	Description
scorecard_file	A comma delimited list of object_stage (.cmo) files that contain the scorecards from the earlier version of Metrics Manager. The list must include all of the scorecards that you want to import into the Cognos 8 metric store. Only scorecards are imported; other objects in these files are ignored.
policy_file	A comma delimited list of source object_link_stage (.cml) files from the earlier version of Metrics Manager that contain the policies to be upgraded. The list of files must contain all of the policy links that you want to import into the Cognos 8 metric store. Only policy links are imported; other objects in these files are ignored.
input_file_encoding	The character set of the input files. This property is optional. By default, the default character set of the platform is used.
flat_file_version	The version of the flat file from the earlier version of Metrics Manager. The value may be 2.0 or 2.2. This property is optional. The default value is 2.2.
output_file	The name of the file where the generated Cognos 8 policies will be written. This property is optional. The default output file name is policies.cms.

Property	Description
output_file_encoding	The desired character set of the output file. This property is optional. By default, the default character set of the platform is used.
read_mapping	A comma delimited list of Cognos 8 permissions to grant for the read permission level set in the earlier version of Metrics Manager. One of the following suffixes may be added to specify the permissions for a specific object type: .metric or .scorecard.
write_mapping	A comma delimited list of Cognos 8 permissions to grant for the write permission level set in the earlier version of Metrics Manager One of the following suffixes may be added to specify the permissions for a specific object type: .metric or .scorecard.
administrator_mapping	A comma delimited list of Cognos 8 permissions to grant for the administer permission level set in the earlier version of Metrics Manager. The permissions include: • Read • Write • Setpolicy • Readannotations • Annotate • Writeproject • Writeactual • Writetarget • Writetolerance • Writeudc One of the following suffixes may be added to specify the permissions for a specific object type: .metric or .scorecard.

Example

The following shows an example control file:

```
scorecard_file=c:\\cmm_exports\\export_scorecards.cmo
policy_file=c:\\cmm_exports\\export_permissions.cml
flat_file_version=2.2
```

```
output_file=new_policies.cms
read_mapping=read,readannotations
write_mapping=read,readannotations,annotate,writeProject
administrator_mapping=read,readannotations,annotate,writeProject,write,
  writeactual,writetarget,writetolerance,writeudc
```

Steps

1. Export the contents of the data store from the earlier version of Metrics Manager with the exception of users.

   For more information, see the documentation provided with the earlier version of Metrics Manager.

2. Install Cognos 8:

   - If you are upgrading only Metrics Manager, install Cognos 8 in a different directory from the earlier version of Metrics Manager (p. 93).
   - If ReportNet is on the same computer as Metrics Manager, follow the steps to upgrade ReportNet to Cognos 8 (p. 66).

3. Set up the environment (p. 117).

   Ensure that you create a metric store database (p. 118) and set up the metric store database client (p. 127) and environment variables on UNIX (p. 130).

   Also, ensure that the Series 7 namespace is configured and available in the Cognos 8 environment.

4. Create a control file that references the object stage (.cmo) files, containing the scorecard definitions, and the object link stage (.cml) files, containing the permission definitions generated in step 1.

   The control file is a text file. See the table and example above to help you create your control file.

5. In the *c8_location*\bin directory, type the following command from a command prompt:

   cmm_migrate_policies *control_file_name*

6. Create a metric package (p. 154).

7. Import the data store export you created in step 1 into the metric store.

   You do not have to import the object link stage (.cml) files containing the permission definitions. In the example above, the file containing the permission definition is export_permission.cml.

   For more information about importing, see the Metric Studio *User Guide for Authors*.

8. Import the contents of the output file generated using the cmm_migrate_policy command.

   The output file is named new_policies.cms in the example above.

   Ensure that you specify the import source file format to be 8.1.2MR2.

9. Install (p. 111) and configure (p. 188) Metric Designer on Windows.

10. Upgrade Metric Designer projects and extracts (p. 190) as required.

11. When you are ready, stop the earlier version of Metrics Manager and uninstall it as described in the documentation provided with it.

To ensure the security and integrity of Cognos 8, protect the installation directory from unauthorized or inappropriate access.

Upgrading Metrics Manager Custom Calendars

If you want to upgrade a Metrics Manager 2.2 calendar that uses a customized period start date and end date, you must create a standard calendar in Cognos 8 that reflects your custom calendar as closely as possible. You must then export the standard calendar and modify the import time periods file (.cal), import time levels file (.lvl), and time language text file (.tlt) so that the calendar equals your Metrics Manager 2.2 calendar.

Install or Upgrade Third-party Products

When you upgrade Cognos 8, you may need to upgrade to new versions of third-party products, update some components of third-party products, or install additional third-party products to support new features in Cognos 8.

To view a list of third-party products that are used by Cognos 8, see "Verify System Requirements" (p. 94).

To review an up-to-date list of environments supported by Cognos products, such as operating systems, patches, browsers, Web servers, directory servers, database servers, and application servers, visit the Cognos Global Customer Services Web site (http://support.cognos.com).

Step

- If you do not have the supported version of a required third-party product, install or upgrade the product.

  Instructions are provided in this guide for some of the required third-party products:

  - setting up a database client (p. 127)
  - updating the Java environment (p. 131)
  - configuring a Web server (p. 132)
  - configuring a Web browser (p. 135)
  - changing the type of Java Virtual Machine (JVM) used in Cognos 8 (p. 313)
  - changing the version of Java Runtime Environment used in Cognos 8 (p. 314)

  For instructions to install or upgrade other third-party products, see the instructions provided with each product.

Run ReportNet and Cognos 8 at the Same Time

You must change the ports and the Web server alias in Cognos 8 if you want to run Cognos 8 and ReportNet, or two versions of Cognos 8, on the same computer and at the same time.

In ReportNet, there is no default cookie path, which means the cookie is sent to all URLs on the Web server. If Cognos 8 uses the same Web server, Cognos 8 will then receive two cam_passport cookies. To prevent this conflict, you must set a cookie path in ReportNet.

Other configuration changes may be required depending on your environment. If you use Portal Services, you must specify the location of the applications.xml file. If you use an ISAPI gateway on an IIS 6.0 Web server, you must isolate the Cognos 8 gateway to prevent a conflict with the ReportNet gateway. You isolate the gateway by setting the application protection for the Web site and virtual directories to High.

Steps for Cognos 8

1. In Cognos 8, start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, under **Dispatcher Settings**, click the value for **Internal dispatcher URI**.
4. Select the port number and then type the new port number.
5. If required, change the port number for the following URIs to match the new port number that you entered for **Internal dispatcher URI**.
   - Under **Dispatcher Settings**, change the port for **External dispatcher URI**.
   - Under **Other URI Settings**, change the port for **Dispatcher URI for external applications** and **Content Manager URIs**.

     Content Manager URIs does not appear on a gateway computer.
6. Under **Gateway Settings**, click the value for **Gateway URI** and ensure that the URI contains the correct Web server alias for Cognos 8.

   For example, replace crn with cognos8.
7. If you are using Portal Services, update the applications.xml file:
   - In the **Explorer** window, click **Environment**, **Portal Services**.
   - In the **Properties** window, ensure that the port number for **Location of Applications.xml** matches the port for the other URI properties.
8. In the **Explorer** window, click **Data Access**, **Content Manager**, **Content Store**.
9. In the **Properties** window, configure Cognos 8 to use the new content store:
   - For **Database name**, specify the name of the new content store.
   - For **User ID and password**, click the edit button and specify the userid and password to access the new content store.
10. If you are running two instances of Cognos 8, change the cookie path for the new version of Cognos 8:

- From the **Actions** menu, click **Edit Global Configuration**.
- In the **Global Configuration** window, click **Cookie Settings**.
- Go to a different path from the one that is used by the older version of Cognos 8.
- Click **OK**.

11. Save the configuration and start Cognos 8.
12. If you use an ISAPI gateway on an IIS 6.0 Web server, change the application protection setting:
    - In IIS Manager, right-click the default Web site and then click **Properties**.
    - Click the **Home Directory** tab.
    - In the **Application Protection** box, click **High** and then click **OK**.
    - Repeat the above three bulleted steps for each of the virtual directories for Cognos 8, clicking the **Virtual Directory** tab instead of the **Home Directory** tab.

    The next time the Cognos 8 gateway is requested, it will run in a separate memory space.

Steps for ReportNet

1. In ReportNet, start Cognos Configuration.
2. Change the cookie path:
    - From the **Actions** menu, click **Edit Global Configuration**.
    - In the **Global Configuration** window, click **Cookie Settings**.
    - Set the path to the installation directory (for example, /crn).
    - Click **OK**.
3. Save the configuration.

You can now run ReportNet and Cognos 8, or two instances of Cognos 8, at the same time.

Note: When you change from the default ports on Windows, the port number is automatically appended to the service name. The service name in Cognos Configuration does not show the port number. You can view the service name and port number under **Services** in your Windows administrative tools.

Manually Uninstall the ReportNet Service on Windows

If the ReportNet service continues to run after you uninstalled ReportNet and then installed Cognos 8, you must manually uninstall the ReportNet service.

You can install more than one version of Cognos 8 in different locations on the same computer. If the versions use the same ports, the installation may not upgrade the service correctly. Cognos Configuration upgrades to the most recently configured service for Cognos 8.

Tip: To see if the correct Cognos 8 service is running, check the version number in the **About** window in Cognos Configuration.

Steps

1. Start Cognos Configuration.
2. Right-click the service node **Cognos 8** (or other name that has been given to the service) in the **Explorer** panel and select **Stop**.
3. Open a **Command Prompt** window.
4. Go to the *c8_location*/bin directory.
5. Uninstall the service:
   - If you used the default name for the service, type **cogbootstrapservice -u**
   - If you specified another name, type **cogbootstrapservice -u -name="*c8_service_name*"**
6. Close the **Command Prompt** window.
7. Restart Cognos Configuration.

Cognos 8 upgrades to the correct service.

Set Up to Publish Series 7 PowerCubes After Upgrade from ReportNet

After you upgrade from Cognos ReportNet to Cognos 8, you may not be able to publish cubes from PowerPlay Enterprise Server to Cognos Connection. Similarly, if a user opens a cube from Cognos Connection that was published from PowerPlay Enterprise Server, they may receive the following error when they save the report to Cognos Connection:

Your session ticket is invalid. It may have expired.

To enable publishing of Series 7 PowerCubes after upgrading, you can either restructure your virtual directories so that the Series 7 and Cognos 8 gateways are within the same structure or change the default cookie path in Cognos 8 to the value specified below. If you use the specified cookie path value, you cannot run ReportNet and Cognos 8 on the same computer.

Step to Restructure Virtual Directories

- Create a virtual directory structure where both the PowerPlay Enterprise Server Series 7 gateway and the Cognos 8 gateway are within the same structure. For example, set up your virtual directories as follows:
  - Create an alias called **cognos8** that points to the *c8_location*\webcontent directory.
  - Create an alias called **cognos8/cgi-bin** that points to the *c8_location*\cgi-bin directory.
  - Create an alias called **cognos8/series7** that points to the *series7_location*\webcontent directory.

- Create an alias called **cognos8/series7/cgi-bin** that points to the *series7_location*\cgi-bin directory.
- Create an alias called **cognos8/series7/help** that points to the *series7_location*\Documentation directory.

Steps to Change the Default Cookie Path

1. Start Cognos Configuration.
2. Click **Actions**, **Edit Global Configuration**, and click the **General** tab.
3. In the **Path** box under **Cookie Setting**, type

   /
4. Click **OK**.
5. Save the configuration.

   Note: If you change the cookie path to the specified value, you cannot run ReportNet and Cognos 8 on the same computer. If you intend to run ReportNet and Cognos 8 on the same computer, correct this problem by changing your virtual directories as described above.

Upgrading Cognos 8 Go! Office

To upgrade Cognos 8 Go! Office, users of the client components must first uninstall the older version and then run a setup file that installs a new version of Microsoft .NET Framework, updates the .NET components, and installs the new version of Cognos 8 Go! Office. To upgrade reports, users must open them in the new version and then save them.

There is no action required to update the server components for Cognos 8 Go! Office. They are included in the upgrade to the new version of Cognos 8.

To support the addition of other Cognos products that work with Microsoft Office, the name used to install the new product is now Cognos 8 for Microsoft Office. This name is used in the installation wizard and in the name of the action pane that appears in your Microsoft Office product after upgrading. In addition, the name of the default installation directory is changed to Cognos 8 for Microsoft Office.

If you deployed Cognos 8 Go! Office enabled files or templates, you do not have to revise the custom properties in the new version. The custom properties and templates are no longer required.

Uninstall the Previous Version

Before you can upgrade to the new version of Cognos 8 Go! Office, you must uninstall the old version.

Steps

1. From the **Start** menu, click **Settings**, **Control Panel**.

2. Start **Add or Remove Programs**.
3. In the list of currently installed programs, click **Cognos 8 Go! Office**.
4. Click **Remove** and follow the instructions.

Install Microsoft .NET Framework and the New Version of Cognos 8 Go! Office

To install Microsoft .NET Framework and Cognos 8 for Microsoft Office, you run a setup.exe file from a central LAN location. The file installs and updates your Microsoft .NET Framework, installs the Primary Interop Assemblies (PIAs) that are required by Microsoft Office, and installs the Cognos 8 for Microsoft Office components.

When you install Microsoft .NET Framework in a non-English operating system, Microsoft .NET error messages, shortcuts, and utilities appear in English.

For a language other than English, you can apply the Microsoft .NET Framework Language Pack to view error messages, shortcuts, and utilities in your language. For example, if your operating system is French and you installed Microsoft .NET Framework, you must also apply Microsoft .NET French Language Pack. You can download .NET Framework Version 2.0 Language Pack from http://www.microsoft.com/downloads/.

Before you update and install components, ensure that you

- have administrative privileges on the computer
- uninstalled the previous version of Cognos 8 Go! Office
- have the appropriate license to use Cognos 8 Go! Office

Steps

1. From the LAN location, run the setup.exe file.

   The installation wizard checks whether Microsoft .NET Framework is installed.

2. If the **Cognos 8 for Microsoft Office Setup** dialog box shows the License Agreement page for Microsoft .NET Framework 2.0, click **Accept**.
3. In the **Cognos 8 for Microsoft Office Setup** dialog box, click **Install**.

   If Microsoft .NET Framework is being installed, a progress dialog appears while the files are downloaded from the Microsoft download Web site and then installed. This may take several minutes.

   A progress dialog appears while the shared add-in support update for Microsoft .NET Framework is installed. When the update is complete, the Cognos 8 for Microsoft Office setup Wizard appears.

4. In the **Welcome to the Cognos 8 for Microsoft Office Setup Wizard** page of the Cognos 8 for Microsoft Office window, click **Next**.
5. In the **License Agreement** page, select **I Agree** and then click **Next**.
6. In the **Select Installation Folder** page, do the following:

- Select the installation directory that you used for the old version, such as C:\Program Files\Cognos\Cognos Office\.
- Select **Everyone**.

  When you select **Everyone**, all users who log on to the computer will see **Cognos 8** in the toolbar of the Microsoft Office products. If you select **Just Me**, only the user who installed Cognos 8 for Microsoft Office will see **Cognos 8** in the toolbar.
- Click **Next**.

If a dialog box appears, advising you to uninstall a previous version, follow the prompts and uninstall the previous version, and then resume the installation.

7. In the **Confirm Installation** page, click **Next**.

   The wizard installs the Cognos 8 Go! Office components.
8. In the **Installation Complete** page, click **Close**.
9. To confirm that the installation is successful, do the following:
   - Open Microsoft Office Word, Microsoft Office Excel, or Microsoft Office PowerPoint.
   - Check that **Cognos 8** appears in the toolbar.

     If **Cognos 8** is not in the toolbar, from the **View** menu, click **Toolbars**, **Cognos 8 for Microsoft Office**.
   - Click the **Cognos 8** button in the toolbar.

     The **Cognos 8 for Office** pane appears on the right-hand side of the window. It includes a link to Cognos 8 Go! Office.

Upgrading Transformer Models and PowerCubes

You can open Cognos Series 7 models with secured cubes in Transformer and upgrade the Series 7 user class views and user classes for use in Cognos 8.

Before you load the model, the Cognos Series 7 namespace must be configured in Cognos 8 (p. 263).

To upgrade Transformer models and PowerCubes, do the following:

- ❑ Prepare the Cognos Series 7 models
- ❑ Import unsecured models in Cognos 8 Transformer
- ❑ Upgrade Cognos Series 7 secured PowerCubes in Cognos 8 Transformer

Prepare Models in Cognos Series 7 Transformer

To upgrade models created in earlier versions of Transformer, you must save them in Model Definition Language (MDL) format before you can import them into Transformer 8.3. This ensures

that equivalent definitions are created for all model objects. You can upgrade models from Cognos Series 7 Transformer, versions 7.x.

Ensure that you save all your models as .mdl files before you attempt to upgrade them.

Steps

1. Open the model in the earlier version of Transformer and, from the **File** menu, click **Save As**.
2. In the **Save as Type** box, click **Exported Model Files (*.mdl)**.

   Tip: By default, Transformer saves models in the ../My Documents/Transformer/Models directory. You can set the location to which Transformer saves models by changing the **Models** directory setting on the **Directories** tab of the **Preferences** property sheet.
3. Back up the .mdl files in a secure location.

Import Unsecured Models in Cognos 8 Transformer

After you install Cognos 8 Transformer, you can import the .mdl files from Cognos Series 7 into Cognos 8 Transformer. If you are importing secured models from Cognos Series 7, see the topic about upgrading a Series 7 secured model in Transformer 8.3.

You can open a Cognos Series 7 model with secured cubes in Cognos 8 Transformer, and convert the Series 7 user class views to Cognos 8 custom views. You can then choose the authentication provider you want to use with the custom views. For more information about adding security, see the Transformer *User Guide*.

During the transition from a Cognos Series 7 namespace to an alternate security provider, you can use the PowerCube property **All applicable namespaces (including unsecured PowerCubes)** to associate all applicable namespaces during migration testing. When you associate all the applicable namespaces to the cube, you can ensure that the group, role, or user dimensional filtering is consistent with that which had been applied for the Series 7 user class. This option is supported only for migration testing, and cannot be used to deploy cubes in production environments.

You can change the association for an IQD data source to that of a Cognos 8 data source, thereby taking advantage of the enhancements available when using a Cognos 8 package or report data source. You can change the association for Series 7 .iqd files and for Framework Manager .iqd (externalized query) files, after the updated model has been saved in Transformer 8.3. For more information about changing a data source type, see the Transformer *User Guide*.

Transformer 8.3 supports upgrading models from Cognos Series 7.x. When importing .mdl files from earlier versions, some features may not convert correctly, such as legacy data that contains special characters, spaces, and quotation marks. For more information, see the migration documentation delivered with your version of the product.

Step

- Open the .mdl file in Cognos 8 Transformer, make any required changes to the model design, and save it, again selecting the .mdl format.

When you are ready to use the model in your production environment, you may want to save it as a .py?-format file.

Cognos 8 Transformer models are not backward compatible (.mdl and .pyj). As a result, we strongly recommend that you maintain the .mdl file for the Transformer 7.x model for a period of time following upgrade.

Upgrade a Cognos Series 7 Secured PowerCube

You can open Cognos Series 7 models with secured cubes in Cognos 8 Transformer, and upgrade the Series 7 user class views and user classes for use in Cognos 8.

If you want to move to a Cognos 8 supported authentication provider other than Access Manager, you can do this over time.

When you open the Cognos Series 7 secured model in Cognos 8 Transformer, you can choose to:

- import the Series 7 user class views associated with the model, but not the user classes

  Choose this option when you want to maintain the view operations applied in the Series 7 user class views but not use a Cognos Series 7 namespace with the custom views, or if you do not intend to expose Cognos Series 7 as an available namespace configured in Cognos 8.

  Note: Prior to building and using the Cognos 8 Transformer cube in any of the Cognos 8 Web studios, you will need to associate new security objects to the upgraded custom views.

- import the Series 7 user class views and user classes associated with the model

  Choose this option when you want to maintain the view operations applied in the user class views and use the Cognos Series 7 user classes, or if you want to transition to an alternate security provider but need to maintain the Series 7 user class objects to ensure the transition is carried out correctly.

  This option requires you to configure the Cognos Series 7 security on which the upgraded model was designed as an available namespace in Cognos 8. The unique identifier that locates the user class in Access Manager is converted to a Cognos 8 identifier, and this process will not be successful if you use this option with a different Cognos Series 7 namespace.

- discard all existing custom views and security objects

  Choose this option when you plan to create new custom views and use only the security objects currently configured in the Cognos 8 namespace.

For PowerCubes that are in development and transitioning from a Series 7 namespace to an alternate security provider, you can associate all the applicable namespaces on the PowerCube property sheet (Data Source tab). This option is intended only for the testing of migration, and requires that the modeler or administrator log on to all the applicable namespaces prior to accessing the PowerCube package in Cognos 8. Failing to log on to all applicable namespaces will result in an inaccurate view of the data. This feature is not supported for the deployment of cubes for end users.

For more information about publishing a PowerCube, see the Transformer *User Guide*.

Steps

1. From the **File** menu, click **Open**, browse to the location of the Series 7 secured model, select the model, and then click **Open**.
2. In the **Import model with Cognos Series 7 user class view** dialog box, select the appropriate security import option, and then click **Next**.
3. If you selected **Import user class views and user classes from the model**, in the **Logon** dialog box, select the appropriate namespace and then log on with your user ID and password.
4. In the **Available namespace(s)** box, select the namespace used to secure the Series 7 cube.

   Tip: If the namespace does not appear in the list, click **Logon As** to select and log on to the namespace.
5. Click **Finish**.

Chapter 5: Workflows for Cognos 8

After you decide on the appropriate distribution options (p. 27) for your environment, you must follow a specific workflow to install and configure Cognos 8. For example, follow one workflow to install and configure Cognos 8 on a single computer. Follow another workflow to install and configure Cognos 8 in a distributed installation.

Depending on the Cognos 8 solution purchased by your organization, other Cognos products may be available to you. A separate workflow is provided for each product CD, as follows:

- installing Cognos 8
- adding Framework Manager
- adding Metric Studio
- adding Transformer

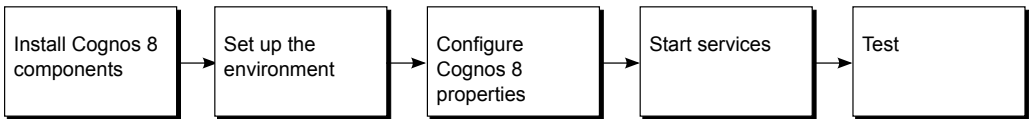
To create PowerCubes, you must also install Transformer after installing Cognos 8 (with or without Metric Studio).

The workflows do not show optional configuration tasks (p. 193) and changing application servers (p. 293).

We recommend that you print the workflow you plan to use. You can then use the printed copy as a checklist to ensure that you have completed all tasks.

The workflows require that you perform tasks in sequence. Many of the tasks you perform for distributed installations are the same as those you perform for single-computer installations. However, additional tasks are required for distributed installations so that the components can communicate with each other.

When you install any Cognos 8 product, the underlying process does not change.



On each computer, you do the following:

- ❑ Install Cognos 8 components.
- ❑ Set up the environment by installing or configuring third-party products.
- ❑ Configure Cognos 8 properties using Cognos Configuration.

  Some tasks may require that you also configure properties for third-party products.
- ❑ Start the Cognos services.

  In a distributed installation, it is important to start the services on the Content Manager computer first, so that cryptographic keys are created and available to other computers.

- Test your Cognos 8 product by using the test feature in Cognos Configuration and performing one or two simple tasks.

Installing Cognos 8

When you install Cognos 8 Business Intelligence, you install the user interfaces for reporting, analysis, and event management, as well as the server functionality for routing and processing user requests. When Cognos 8 is running, you can then add other Cognos 8 interfaces or products to that environment. For example, you can add Metric Studio, the interface for scorecarding.

Two tasks in the workflows, "Create content store database" and "Set up database clients", are not required if you use the Cognos Content Database that is provided with Cognos 8 and you install Cognos 8 components on a single computer. A database is already created and the connection properties are already set for the database in Cognos Configuration. If you use any other type of database for the content store, or if you install Cognos Content Database on a different computer from Content Manager, you must perform these two tasks.

Single-computer Installation

This workflow shows the required tasks for installing and configuring Cognos 8 on a single computer. A single-computer installation is useful for an environment with a small number of users or for testing.

Single Computer

1. Install Cognos 8 (p. 98).
2. Check the default settings (p. 104).
3. Create the content store database (p. 118).
4. Set up the database client (p. 127).
5. Update the Java environment (p. 131).
6. Configure the Web server (p. 132).
7. Configure the Web browsers (p. 135).
8. Configure a user account (p. 137).
9. Set the database connection properties for the content store (p. 147).
10. Configure the mail server account and notification database (p. 149).
11. Start the services (p. 151).
12. Test the installation and configuration (p. 152).
13. Finish the configuration (p. 156).

Distributed Installation

These workflows show the required tasks for installing and configuring Cognos 8 on multiple computers in a distributed environment. The workflows are listed in the order in which the computers must be configured. The components on the Content Manager computer must be installed, configured, and started first. As you add computers to the configuration, each computer then obtains the cryptographic keys from Content Manager.

Content Manager Computer

1. Install Content Manager (p. 98).
2. Check the default settings (p. 104).
3. Create the content store database (p. 118).
4. Set up the database client (p. 127).
5. Update the Java environment (p. 131).
6. Configure a user account (p. 137).
7. Set the database connection properties for the content store (p. 159).
8. Configure the mail server account and notification database (p. 162).
9. Configure the environment and security properties (p. 163).
10. Start the services (p. 191).
11. Test the installation and configuration (p. 192).
12. Finish the configuration by configuring authenticated access (p. 255) or by changing the default settings (p. 193), for example.

Application Tier Components Computer

1. Install Application Tier Components (p. 98).
2. Check the default settings (p. 104).
3. Set up ODBC connections to the data sources (p. 142), if required.
4. Configure the mail server account and notification database (p. 167).
5. Configure the environment and security properties (p. 169).
6. Start the services (p. 191).
7. Test the installation and configuration (p. 192).
8. Finish the configuration (p. 193).

Gateway Computer

1. Install the Gateway (p. 98).

2. Check the default settings (p. 104).
3. Configure the Web server (p. 132).
4. Configure the environment and security properties (p. 171).
5. Start the services (p. 191).
6. Test the installation and configuration (p. 192).
7. Finish the configuration by configuring Cognos 8 Go! Office (p. 237), for example.

Client Computers

1. Deploythe client for Cognos 8 Go! Office (p. 240), if required.
2. Configure the Web browser (p. 135).

Adding Framework Manager to a Cognos 8 Installation

To publish your business-related metadata for use by Cognos 8 reporting tools, you must add Framework Manager to an existing Cognos 8 installation. The following workflow assumes that the Cognos 8 installation is complete.

Framework Manager Installation

1. Ensure that the other Cognos 8 components are installed and working (p. 192).
2. Install Framework Manager on a windows computer (p. 105).
3. Check the default settings (p. 107).
4. For a distributed installation, configure the environment properties (p. 177).
5. Test the installation and configuration (p. 192).
6. Upgrade projects (p. 179), if required.

Adding Metric Studio to a Cognos 8 Installation

You may choose to add Metric Studio, the interface for scorecarding, to an existing Cognos 8 installation. The following workflows show the required tasks for installing and configuring on a single computer and in a distributed installation where a Cognos 8 installation exists. A workflow is also provided for installing and configuring Metric Designer, the modeling tool used to create extracts for use in Metric Studio.

Single-Computer Installation

1. Install Metric Studio and Metric Designer (p. 111)
2. Check the default settings (p. 113).

3. Create the metric store database (p. 124).
4. Set up the database clients (p. 127).
5. Setthe metric store environment variables on UNIX (p. 130).
6. Start the services (p. 151).
7. Create a metric package (p. 154).
8. Test the installation and configuration (p. 152).
9. Finish the configuration (p. 193).

Distributed Installation

1. Install Metric Studio components on two or more computers (p. 111)
2. Check the default settings (p. 113).
3. Create the metric store database (p. 124).
4. Set up the database clients (p. 127).
5. Set the metric store environment variables on UNIX (p. 130).
6. Configure Application Tier Components computers (p. 169).
7. Start the services (p. 191).
8. Create a metric package (p. 174).
9. Test the installation and configuration (p. 192).
10. Finish the configuration (p. 193).

Metric Designer Installation

1. Ensure that the other Cognos 8 components are installed and working.
2. Ensure that the applications associated with the metadata sources are installed and running.
3. Install Metric Designer on a Windows computer (p. 111).

   In addition to the Metric Studio computers where Application Tier Components are installed, Metric Studio Application Tier Components must also be installed on all computers where Application Tier Components for other Cognos 8 products are installed.
4. Check the default settings (p. 113).
5. For a distributed installation, configure the environment properties (p. 189).
6. Start the services (p. 191).
7. Upgrade projects (p. 190), if required.

Adding Transformer to a Cognos 8 Installation

To create PowerCubes, you must add Transformer to an existing Cognos 8 installation. The following workflow assumes that the Cognos 8 installation is complete.

Cognos 8 Transformer Installation

1. Ensure that the other Cognos 8 components are installed and working.
2. Install Cognos 8 Transformer (p. 108).
3. Check the default settings (p. 111).
4. For a distributed installation, install the database client software on the Transformer computer (p. 127).
5. For a distributed installation, configure the environment properties (p. 181).
6. Test the installation and configuration (p. 192).

Chapter 6: Installing Cognos 8

If you plan to install two or more Cognos 8 components on the same computer, we strongly recommend that you install them in the same installation location to avoid conflicts among ports and other default settings.

If you are installing Cognos 8 in an application server environment, you must be aware of the installation requirements. For more information, see "Configuring Cognos 8 for a Third-Party Application Server" (p. 293).

If you are upgrading from a previous release of Cognos products, you must use the upgrading steps. For information about upgrading from ReportNet or Metrics Manager, see "Upgrading to Cognos 8" (p. 49).

Use the following checklist to guide you through the installation tasks:

- ❑ Review the Readme
- ❑ Ensure that your computer meets the software and hardware requirements
- ❑ Set up database connectivity for the reporting database
- ❑ Set up database connectivity for the content store database
- ❑ Set up database connectivity for the metric store database
- ❑ Review the supported environments
- ❑ Install the server components
- ❑ Install Framework Manager
- ❑ Install Cognos 8 Transformer
- ❑ Install Metric Designer

After you install Cognos 8, you must set up your environment.

This chapter also includes information for uninstalling Cognos 8. For more information, see "Uninstalling Cognos 8" (p. 113).

Recommendation - Review the Readme Before You Install

Before you install your Cognos product, it is important to be aware of all issues that may affect your installation strategy.

There may be late-breaking issues that were not known when this installation guide was created.

We recommend that you review the readme before you install your product. The readme contains late-breaking information about known issues as well as documentation updates and deprecation

notices. The readme is available from the first page of the installation wizard or from the product CD.

Verify System Requirements

Use the following table to check the minimum hardware and software requirements to install and run Cognos 8 components on one computer. Additional resources may be required for distributed or production environments.

Requirement	Specification
Operating system	Windows UNIX: • Sun Solaris • HP-UX • IBM AIX Linux Some Cognos 8 components are not supported under Linux.
RAM	Minimum: 2 GB
Operating system specifications	File descriptor limit set to 1024 on Solaris (recommended)
Disk space	A minimum of 2.5 GB of free space is required to install the software and 1 GB of free space on the drive that contains the temporary directory used by Cognos components. For Metric Studio, the size of the metric store will increase over time. Ensure that you have sufficient disk space for future requirements.
Web server	A Web server must be installed and started.

Requirement	Specification
JRE	Java Runtime Environment (JRE) JRE is installed automatically with Cognos 8 on Windows. If you are using an application server, use the JRE that is installed with it, if it is supported in Cognos 8.
Database	Cognos Content Database can be installed and configured as the default content store database. If you want to use another database, you must have one of the following databases available to store Cognos data: • Oracle • DB2 • Microsoft SQL Server TCP/IP connectivity to Microsoft SQL Server • Sybase For Metric Studio, the following databases are supported for the metric store: • Oracle • DB2 • Microsoft SQL Server TCP/IP connectivity to Microsoft SQL Server

Requirement	Specification
Web browser	For all Web browsers, the following are enabled: • cookies • JavaScript For Microsoft Internet Explorer only, the following are enabled: • Run ActiveX controls and plug-ins • Script ActiveX controls marked safe for scripting • Active scripting • Allow META REFRESH
Other	For a terminal emulator to install Cognos 8 on UNIX, the emulation set to VT220 equivalent or better to ensure that the hot keys in the Installation wizard work On Windows, Microsoft Data Access Component (MDAC) for use with product samples If you want to email reports, the ability to use a mail server
SAP BW	The following SAP Front-End components installed on each Cognos 8 server computer: • SAP GUI • BW Add-ons

Set Up Database Connectivity for the Reporting Database

For Cognos 8, the only service that accesses the query database (also known as reporting database) is the reporting engine that runs reports.

To set up database connectivity for the reporting database:

- Ensure that you install the database API software for your reporting sources on each Cognos 8 server computer.

On Windows, the report server supports either native database connectivity or ODBC. On UNIX and Linux, the report server supports the native database connectivity.

On UNIX, for Microsoft SQL Server only, the report server supports the Data Direct ODBC driver. This driver is available from Data Direct.

Cognos 8 requires TCP/IP connectivity with the Microsoft SQL Server.

Set Up Database Connectivity for the Content Store Database

If you are using a database other than Cognos Content Database as the content store, database client software must be installed and configured on each computer where you install Content Manager.

To set up database connectivity for the content store database:

- Install the appropriate JDBC driver for your Content Manager database, as follows:

Database	JDBC Driver
Oracle	JDBC thin driver, ojdbc14.jar If the directory contains the classes12.jar file, you must delete it before installing the ojdbc14.jar file.
DB2	JDBC driver that requires DB2 client installation
Microsoft SQL Server	Included with Cognos components. No other software is required. Cognos 8 requires TCP/IP connectivity with Microsoft SQL Server.
Sybase	JDBC driver, jconn2.jar
Cognos Content Database	Included with Cognos components. No other software is required.

Set Up Database Connectivity for the Metric Store Database

For Metric Studio, the Application Tier Components must be able to access the metric store. The database client software for the metric store must be installed and configured on each computer where you install Application Tier Components.

To set up database connectivity for the metric store database:

- Install the appropriate JDBC driver.

Database	JDBC Driver
Oracle	JDBC OCI driver
DB2	JDBC driver that requires DB2 client installation
Microsoft SQL Server	Included with Cognos components. No other software is required. Cognos 8 requires TCP/IP connectivity with Microsoft SQL Server.

Review Supported Environments

To ensure your product works properly, apply all required operating system patches and use only the versions of third-party software that are supported for a Cognos product.

To review an up-to-date list of environments supported by Cognos products, such as operating systems, patches, browsers, Web servers, directory servers, database servers, and application servers:

- Visit the Cognos Global Customer Services Web site (http://support.cognos.com).

  It is important to note that the Linux operating system is available in a number of distributions and supports a number of hardware platforms. Ensure that the operating system and hardware combination you are using is a supported combination.

  When you install Cognos 8 on Linux, Framework Manager is not installed. The BMTScriptPlayer is a command-line utility that interfaces with the Framework Manager engine, allowing you to run Framework Manager action logs. Because Framework Manager is not installed, the BMTScriptPlayer will not work.

Install Server Components

Use the installation wizard to select the server components that you want to install and the location on your computer where you want to install them. Only the components that you choose to install are copied from the CD to your computer. You can install the gateway, Application Tier Components, and Content Manager components on multiple computers.

In previous versions of Cognos 8, the samples were installed automatically with the server components. Now the samples are on a separate CD in your Cognos 8 product. If you want to use the samples, you must install them from the Cognos 8 Business Intelligence Samples 8.3 CD. For more information, see "Install the Cognos 8 Samples" (p. 102).

For instructions about installing Framework Manager, see "Install Framework Manager" (p. 105).

For instructions about installing Metric Designer, see "Install Metric Designer" (p. 111).

For instructions about installing Cognos 8 Transformer, see "Install Cognos 8 Transformer" (p. 108).

In you are upgrading Cognos 8 BI in an environment that includes earlier versions of other Cognos 8 products, such as Cognos 8 Controller 8.2, Cognos 8 Planning 8.2, or Cognos 8 BI Analysis for Excel 8.2, install the new version of Cognos 8 BI in a separate location from the other Cognos 8 product and configure Cognos 8 BI to operate independently of that product. After you upgrade the other product to a compatible version with Cognos 8 BI, you can then configure the two products to operate together.

If you want to use Cognos Content Database as your content store, you must select it in the installation wizard. If you are installing components on several computers, you need to only install one Cognos Content Database. If you install Cognos Content Database on the same computer as Content Manager, and you later decide to use another database for your content store, you must uninstall Cognos Content Database.

On UNIX, you can install server components using either a character-based interface or a graphical user interface. To run graphical-mode installation, the console attached to your UNIX computer must support a Java-based graphical user interface.

On UNIX, Cognos 8 respects the file mode creation mask (umask) of the account running the installation program. This affects only the installation directories. It does not affect the file permissions within the directories. However, run-time generated files, such as logs, respect the mask. We recommend umask 022 on the installation directory.

On Windows, ensure that you have administrator privileges for the Windows computer you are installing on. Also ensure that your computer has a TEMP system variable that points to the directory where you want to store temporary files. During installation, files from the CD are temporarily copied to this directory.

If you plan to install Cognos 8 Transformer and you will be using PowerCubes that are secured against a Cognos Series 7 namespace, you must install Content Manager on a computer that supports Cognos Series 7.

Important: For successful failover between Content Managers, ensure that the system clocks on the Content Manager computers are synchronized.

Steps for UNIX and Linux

1. If you are installing to a directory with other Cognos 8 components, stop the Cognos 8 service.
2. Set the JAVA_HOME environment variable to point to the installation location of your Java Runtime Environment (JRE).

   An example of the installation location of a Java Runtime Environment is /directory/java/*java_version*/jre.

   Cognos 8 requires Sun Java to run on Linux.
3. On HP-UX, set the _M_ARENA_OPTS environment variable as follows:

   _M_ARENA_OPTS 1:4

This increases the memory allocation for HP-UX to more closely match that of other UNIX platforms.

4. On AIX, set the AIXTHREAD_SCOPE environment variable as follows:

   AIXTHREAD_SCOPE=S

   This sets the contention scope for user threads to system-wide, which supports more efficient scheduling of user threads.

5. Mount the CD for your Cognos product using Rock Ridge file extensions.

   Important: To mount the Cognos CD on HP-UX, do the following:

   - Add the pfs_mount directory in your path.

     For example,

     PATH=/usr/sbin/:$PATH

     export PATH

   - To start the required NFS daemons and run the daemons in the background, type **bg pfs_mountd** and then type **bg pfsd**

   - To mount the drive, type

     pfs_mount -t rrip <device><mount_dir> -o xlat=unix

     For example,

     pfs_mount /dev/dsk/c0t2d0 /cdrom -o xlat=unix

     You can now install or copy files as a non-root user using a Cognos CD from this drive.

   - When the installation is complete, type **pfs_umount /cdrom** and kill the pfsd and pfs_mountd daemons to unmount the CD.

6. Go to the directory on the CD that is appropriate for your operating system.

   For example, for Solaris, go to the solaris directory.

7. Start the installation wizard:

   - If you use XWindows, type

     ./issetup

     Note: When you use the issetup command with XWindows, Japanese characters may be corrupted. When installing on UNIX, use the console display to install components and specify English-only for the installation by setting LANG=C and LC_ALL=C.

   - If you do not use XWindows, type

     ./issetupcc

8. Follow the directions in the installation wizard and copy the required files to your computer.

   Install Cognos 8 components in a directory that contains only ASCII characters in the path name. Some UNIX and Linux Web servers do not support non-ASCII characters in directory names.

If you are installing Cognos 8 on a computer that already has ReportNet and you want to keep the ReportNet, you must install Cognos 8 in a different directory.

If you are installing it in a directory that contains other Cognos 8 components, you are prompted for the location of a directory in which to store backup copies of the files that will be overwritten.

9. Choose how to proceed in the **Finish** page of the installation wizard:
   - We recommend that you do not configure Cognos 8 immediately because you must do other tasks first to ensure that your environment is properly set up. However, if you do not plan to install the Cognos 8 samples and the console attached to your computer supports a Java-based graphical user interface, you can click **Start Cognos Configuration**.
   - If you want to see late-breaking information about Cognos 8, select **View the Readme** and then click **Finish**.

     Tip: For character-mode installations on UNIX and Linux, close the readme text file by pressing Ctrl + C or Q.
   - If the console attached to your computer does not support a Java-based graphical user interface or if you plan to install the Cognos 8 samples, click **Finish**.

     You can later configure Cognos 8 using Cognos Configuration by starting cogconfig.sh in the *c8_location*/bin directory, or editing cogstartup.xml in *c8_location*/configuration directory.
10. Append the *c8_location*/bin directory to the appropriate library path environment variable.
    - For Solaris and Linux, LD_LIBRARY_PATH
    - For AIX, LIBPATH
    - For HP-UX, SHLIB_PATH
11. On Linux, set the PRINTER environment variable to the name of your printer.

To ensure the security and integrity of Cognos 8, it is important to protect the installation directory from unauthorized or inappropriate access.

If you want to use the samples that are available for Cognos 8, install the Cognos 8 samples.

If you use Oracle, DB2, or Sybase you can now set up the database client for the content store and the metric store (p. 127). If you have installed Cognos Content Database, you do not have to set up the database client.

You must also update your Java security framework (p. 131) before you can configure Cognos 8. Otherwise, you may receive the following error:

```
[Cryptography]
1. [ ERROR ] java.lang.NoClassDefFoundError:
javax/net/ServerSocketFactory:
```

Steps for Windows

1. If you are installing to a directory with other Cognos 8 components, stop the Cognos 8 service.

2. Insert the CD for your Cognos product.

   The **Welcome** page of the installation wizard should appear.

   If no **Welcome** page appears, in the win32 directory on the CD, double-click the issetup.exe file.

3. Select the language to use for the installation.

   The language that you select determines the language of the user interface. You can change the language to any of the installed languages after installation.

4. Follow the directions in the installation wizard to copy the required files to your computer.

   If you are installing Cognos 8 on a computer that already has ReportNet, and you want to keep ReportNet running, you must install Cognos 8 in a different directory.

   If you are installing in a directory that contains other Cognos 8 components, you are prompted for the location of a directory in which to store backup copies of the files that will be overwritten.

5. In the **Finish** page of the installation wizard,

   - If you do not plan to install the Cognos 8 samples and want to configure Cognos components immediately, click **Start Cognos Configuration**.
   - If you want to see late-breaking information about Cognos components, click **View the Readme**.

6. Click **Finish**.

   Use the Windows **Start** menu to start **Cognos Configuration** from the shortcut folder.

If you want to use the samples that are available for Cognos 8, install the Cognos 8 samples. If you use Oracle, DB2, or Sybase you can now set up the database client for the content store and the metric store (p. 127). If you have installed Cognos Content Database, you do not have to set up the database client.

Install the Cognos 8 Samples

The Cognos 8 samples illustrate product features and technical and business best practices. You can also use them for experimenting with and sharing report design techniques, and for troubleshooting. If you want to use the samples, install them from the Cognos 8 Business Intelligence Samples 8.3 CD.

Steps for UNIX and Linux

1. Mount the CD using Rock Ridge file extensions.

   Important: To mount the Cognos CD on HP-UX, do the following:

   - Add the pfs_mount directory in your path.

     For example,

     PATH=/usr/sbin/:$PATH

     export PATH

- To start the required NFS daemons and run the daemons in the background, type **bg pfs_mountd** and then type **bg pfsd**
- To mount the drive, type

  pfs_mount -t rrip <device><mount_dir> -o xlat=unix

  For example,

  pfs_mount /dev/dsk/c0t2d0 /cdrom -o xlat=unix

  You can now install or copy files as a non-root user using a Cognos CD from this drive.
- When the installation is complete, type **pfs_umount /cdrom** and kill the pfsd and pfs_mountd daemons to unmount the CD.

2. Go to the directory on the CD that is appropriate for your operating system.
3. Start the installation wizard:
   - If you use XWindows, type

     ./issetup

     Note: When you use the issetup command with XWindows, Japanese characters may be corrupted. When installing on UNIX, use the console display to install components and specify English-only for the installation by setting LANG=C and LC_ALL=C.
   - If you do not use XWindows, type

     ./issetupcc
4. Follow the directions in the installation wizard and copy the required files to your computer.

   Install the samples in the same location as the server components.
5. In the **Finish** page of the installation wizard, click **Finish**.

To set up and configure the Cognos 8 samples, see "Setting Up the Samples" (p. 328).

Steps for Windows

1. Insert the CD.
2. Go to the directory on the CD that is appropriate for your operating system.
3. Start the installation wizard by clicking issetup.exe.

   The **Welcome** page of the installation wizard should appear.
4. Select the language to use for the installation.

   The language that you select determines the language of the user interface. You can change the language to any of the installed languages after installation.
5. Follow the directions in the installation wizard to copy the required files to your computer.

   Install the samples in the same location as the server components.
6. In the **Finish** page of the installation wizard, click **Finish**.

7. Click **Finish**.

   Use the Windows **Start** menu to start **Cognos Configuration** from the shortcut folder.

To set up and configure the Cognos 8 samples, see "Setting Up the Samples" (p. 328).

Default Settings for Cognos 8

The following table lists the default ports and URI settings for Cognos 8. After installation, you can use the configuration tool to change the settings (p. 196). You can also change them by editing the cogstartup.xml file in the *c8_location*\configuration directory.

Setting	Default	Description
Content Manager URI	http://localhost:9300/p2pd/servlet	The URI to Content Manager
Gateway URI	http://localhost:80/cognos8/cgi-bin/ cognos.cgi	The URI to the gateway
Dispatcher URI (Internal, External)	http://localhost:9300/p2pd/servlet/dispatch	The URI to the dispatcher
Dispatcher URI for external applications	http://localhost:9300/p2pd/servlet/dispatch	The URI to the dispatcher
Dispatcher URIs for Gateway	http://localhost:9300/p2pd/servlet/dispatch/ ext	The URI to the primary dispatcher used by the gateway
Log server port	9362	The port used by the local log server
Listening port number	1527	The port used by Cognos Content Database.

The following table lists the default settings used by Cognos 8 for Tomcat. The non-SSL and SSL connectors are automatically updated in the server.xml file when you use Cognos Configuration to change the dispatcher port (p. 196) or to enable the SSL protocol (p. 211). You can directly update the shutdown port using Cognos Configuration.

Setting	Port	Description
Non-SSL Coyote HTTP/ 1.1 Connector	9300	The port Tomcat uses to pass requests from the Web server to Cognos 8
SSL Coyote HTTP/1.1 connector	9334	The port Tomcat uses to listen for secure connections
Shutdown port	9399	The port Tomcat uses to listen for a shutdown command

Install Framework Manager

You can install Framework Manager, the metadata modeling tool for Cognos 8 for reporting, on the same computer as other Cognos 8 components, or on a different computer. All required files are copied to one computer. Default settings are used for the configuration. You can change these default settings if necessary, or if you install Framework Manager on a separate computer from Cognos 8.

If you are upgrading Framework Manager from an older version, you must first uninstall the older version of Framework Manager (p. 114).

Before you install Framework Manager, we recommend that you close all programs that are currently running to ensure that the installation program copies all the required files to your computer.

Also, ensure that you have administrator privileges for the Windows computer you are installing on. If you are not an administrator, ask your system administrator to add you to the Administrator group on your computer. Administrator privileges are also required for the account that is used to run Framework Manager.

We recommend that you install and configure all Cognos 8 server components before you install Framework Manager.

If you are installing the modeling tool in the same directory as Cognos 8 and do not stop the Cognos 8 services, you are prompted to do so during the installation.

System Requirements for Framework Manager

Before you install Framework Manager, ensure that the Windows computer meets Cognos 8 software and hardware requirements. The size of your models determines the hardware requirements, such as disk space.

The following table lists the minimum hardware and software requirements to run Framework Manager.

Requirement	Specification
Operating system	Windows
RAM	Minimum: 512 MB Recommended: 1 GB
Disk space	Minimum: 500 MB of free space on the drive that contains the temporary directory used by Cognos 8
Database	Database client software installed on the same computer as Framework Manager (Oracle, DB2, or Sybase only) Database connectivity set up
Other	Microsoft Data Access Component (MDAC) 2.6 or later for use with product samples

Steps

1. If you use an Oracle database as a data source for your reports, set the NLS_LANG environment variable by typing the following command on each computer where Framework Manager and the Application Tier Components are installed:

   NLS_LANG = language_territory.character_set

   For example, NLS_LANG = JAPANESE_JAPAN.UTF8

   The value of the variable determines the locale-dependent behavior of Cognos 8. Error messages, sort order, date, time, monetary, numeric, and calendar conventions automatically adapt to the native language and locale.

   If the Application Tier Components are installed on a UNIX computer, the NLS_LANG variable must be set up for the user who owns and starts the Cognos 8 service.

2. If you are installing in a directory with other Cognos 8 components, stop the Cognos 8 service.

3. Insert the CD for Framework Manager.

   The **Welcome** page of the installation wizard should appear.

   If no **Welcome** page appears, in the win32 directory on the CD, double-click the issetup.exe file.

4. Select the language to use for the installation.

The language that you select determines the language of the user interface. You can change the language to any of the installed languages after installation.

5. Follow the directions in the installation wizard to copy the required files to your computer.

   If you are installing Cognos 8 on a computer that already has ReportNet, and you want to keep ReportNet running, you must install Cognos 8 in a different directory.

   If you are installing in a directory that contains other Cognos 8 components, you are prompted for the location of a directory in which to store backup copies of the files that will be overwritten.

6. In the **Finish** page of the installation wizard,

   - If you do not plan to install the Cognos 8 samples and want to configure Cognos components immediately, click **Start Cognos Configuration**.
   - If you want to see late-breaking information about Cognos components, click **View the Readme**.

7. Click **Finish**.

   Use the Windows **Start** menu to start **Cognos Configuration** from the shortcut folder.

To ensure the security and integrity of Cognos 8, it is important to protect the installation directory from unauthorized or inappropriate access.

If you use Oracle, DB2, or Sybase as the database server for the content store in a distributed installation, you must now install the database client software (p. 127) on the same computer where you installed Framework Manager.

After you install Framework Manager on your Windows computer, some configuration tasks may be required to ensure that it works in your reporting environment (p. 176).

Default Settings for Framework Manager

The following table lists the default settings for the Cognos 8 ports and URIs that are used by Framework Manager. After installation, you can use the configuration tool to change the settings. You can also change them by editing the cogstartup.xml file in the *c8_location*\configuration directory.

Component	Default	Description
Gateway	http://localhost:80/ cognos8/cgi-bin/ cognos.cgi	The URI to the Cognos 8 gateway
Dispatcher URI for external applications	http://localhost:9300/ p2pd/servlet/dispatch	The URI to the dispatcher
Log Server Port	9362	The port used by the local log server

Install Cognos 8 Transformer

You can install Cognos 8 Transformer, the metadata modeling tool for creating PowerCubes for use with Cognos 8, on the same computer as other Cognos 8 components, or on a different computer. You can install Cognos 8 Transformer on the same computer as Cognos Series 7 Transformer.

Transformer can now be made available more easily for business specialists who want to design models and build PowerCubes for their own use. For example, IT departments can provide business specialists or Transformer modelers with a Web-based, downloadable installation program from a corporate or secured portal, allowing for easy distribution of the installation files. For more information, see "Create a Network Installation Location for Transformer Modelers" (p. 185) and "Deploying Cognos 8 Transformer for Modelers" (p. 187).

If you install Cognos 8 Transformer on the same Windows computer as other Cognos 8 components, all required files are copied to one computer. Default settings are used for the configuration. You can change these default settings if necessary, or if you install Cognos 8 Transformer on a separate computer from Cognos 8.

If you will be using PowerCubes that are secured against a Cognos Series 7 namespace, Content Manager must be installed on a computer that supports Cognos Series 7.

When you select a language in the installation wizard, it determines the language of the user interface. Only that language is installed. You cannot change the language properties after installation. If you want to change the language of the user interface, you must reinstall Cognos 8 Transformer.

For a complete UNIX or Linux installation of Cognos 8 Transformer, you must install client components on a Windows computer and server components on UNIX or Linux computers. The Cognos 8 Transformer client provides a graphical user interface for use on Windows computers. You then build cubes on your UNIX or Linux computer. On Linux, models must contain a Cognos 8 package query as a data source. Models that contain a Cognos Series 7 data source are not supported on Linux.

Before you install Cognos 8 Transformer, we recommend that you close all programs that are currently running to ensure that the installation program copies all the required files to your computer.

If you are installing on Windows, ensure that you have administrator privileges for the Windows computer you are installing on. If you are not an administrator, ask your system administrator to add you to the Administrator group on your computer.

Note: When Transformer 8.3 is installed on Windows Vista, if you do not have Administrator privileges on the computer and you make changes to the cogtr.xml file, the updated file is saved by default to a Virtual Store directory and not to the *c8_location*/configuration directory.

You must install and configure all Cognos 8 server components before you install Cognos 8 Transformer.

System Requirements for Cognos 8 Transformer

Before you install Cognos 8 Transformer, ensure that the computer meets Cognos 8 software and hardware requirements. The size of your PowerCubes determines the hardware requirements, such as disk space.

The following table lists the minimum hardware and software requirements to run Cognos 8 Transformer.

Requirement	Specification
Operating system	Windows UNIX: Sun Solaris, HP-UX, IBM AIX Linux
RAM	Minimum: 512 MB Recommended: 1 GB
Disk space	Minimum: 500 MB of free space on the drive that contains the temporary directory used by Cognos 8
Data source	Database client software installed on the same computer as Cognos 8 Transformer Database connectivity set up
Other	Microsoft Data Access Component (MDAC) 2.6 or later for use with product samples

Steps for UNIX or Linux

1. Insert the CD for Cognos 8 Transformer into the UNIX or Linux computer.
2. To start the installation, type **./issetup**
3. Follow the directions in the installation wizard and copy the required files to your computer.

   Tip: The Series 7 IQD Bridge component is not supported on Linux and HP-UX Itanium.
4. Choose how to proceed in the **Finish** page of the installation wizard:
   - We recommend that you do not configure Cognos 8 Transformer immediately because you must do other tasks first to ensure that your environment is properly set up. However, if you want to begin configuration immediately and the console attached to your computer supports a Java-based graphical user interface, you can click **Start Cognos Configuration**.
   - If you want to see late-breaking information about Cognos 8 Transformer, select **View the Readme** and then click **Finish**.

Tip: For character-mode installations on UNIX and Linux, close the readme text file by pressing Ctrl + C or Q.

- If the console attached to your computer does not support a Java-based graphical user interface or if you want to configure Cognos 8 Transformer later, click **Finish**.

  You can later configure Cognos 8 Transformer using Cognos Configuration by starting cogconfig.sh in the *c8_location*/bin directory, or editing cogstartup.xml in *c8_location*/configuration directory.

5. Create a MANPATH environment variable and configure it to point to the cogtr.1 file in the *c8_location*/webcontent/documentation/en directory.

   The cogtr.1 file provides the syntax for UNIX command line options that are supported by Cognos 8 Transformer. The man page is accessible in UNIX by typing **man**.

To ensure the security and integrity of Cognos 8, it is important to protect the installation directory from unauthorized or inappropriate access.

If you use Oracle, DB2, or Sybase as the database server for the content store in a distributed installation, you must now install the database client software (p. 127) on the same computer where you installed Cognos 8 Transformer.

Steps for Windows

1. Insert the CD for Cognos 8 Transformer modeling product.

   The **Welcome** page of the installation wizard should appear.

   If no **Welcome** page appears, in the win32 directory on the CD, double-click the issetup.exe file.

2. Select the language to use for the installation.

   The language that you select determines the language of the user interface. You cannot change the language after installation because only the selected language is installed.

3. Follow the directions in the installation wizard to copy the required files to your computer.

   If you are installing Cognos 8 on a computer that already has ReportNet, and you want to keep ReportNet running, you must install Cognos 8 in a different directory.

   If you are installing in a directory that contains other Cognos 8 components, you are prompted for the location of a directory in which to store backup copies of the files that will be overwritten.

4. In the **Finish** page of the installation wizard,

   - If you do not plan to install the Cognos 8 samples and want to configure Cognos components immediately, click **Start Cognos Configuration**.

   - If you want to see late-breaking information about Cognos components, click **View the Readme**.

5. Click **Finish**.

   Use the Windows **Start** menu to start **Cognos Configuration** from the shortcut folder.

To ensure the security and integrity of Cognos 8, it is important to protect the installation directory from unauthorized or inappropriate access.

If you use Oracle, DB2, or Sybase as the database server for the content store in a distributed installation, you must now install the database client software (p. 127) on the same computer where you installed Cognos 8 Transformer.

Default Settings for Cognos 8 Transformer

The following table lists the default settings for the Cognos 8 ports and URIs that are used by Cognos 8 Transformer. After installation, you can use the configuration tool to change the settings. You can also change them by editing the cogstartup.xml file in the *c8_location*\configuration directory.

Component	Default	Description
Gateway	http://localhost:80/ cognos8/cgi-bin/ cognos.cgi	The URI to the Cognos 8 gateway
Dispatcher URI for external applications	http://localhost:9300/ p2pd/servlet/dispatch	The URI to the dispatcher

Install Metric Designer

You can install Metric Designer, the metadata modeling tool for Metric Studio, on the same computer as Cognos 8 components, or on a different computer. All required files are copied to one computer. Default settings chosen by Cognos are used for the configuration. However, you may want to change these default settings if existing conditions make the default choices inappropriate, or if you installed Cognos 8 on a different computer.

Before you install Metric Designer, we recommend that you close all programs that are currently running to ensure that the installation program copies all the required files to your computer.

Also, ensure that you have administrator privileges for the Windows computer you are installing on. If you are not an administrator, ask your system administrator to add you to the Administrator group on your computer.

We recommend that you install and configure all Cognos 8 server components before you install Metric Designer.

If you are installing the modeling tool in the same directory as Cognos 8 and do not stop the Cognos 8 services, you are prompted to do so during the installation.

You should also install and configure the target application where you will load data or metadata.

System Requirements for Metric Designer

Before you install Metric Designer, ensure that the Windows computer meets Cognos 8 software and hardware requirements. The size of the your models determines the hardware requirements, such as disk space.

The following table lists the minimum hardware and software requirements to run Metric Designer.

Requirement	Specification
Operating system	Windows (design interface and engine) UNIX (engine only): Sun Solaris HP-UX IBM AIX
RAM	Minimum: 512 MB Recommended: 1 GB
Disk space	Minimum: 500 MB of free space on the drive that contains the temporary directory
Other	Microsoft Data Access Component (MDAC) 2.6 or later for use with product samples

Steps

1. If you are installing in a directory with other Cognos 8 components, stop the Cognos 8 service.
2. Insert the CD for Metric Designer.

   The **Welcome** page of the installation wizard should appear.

   If no **Welcome** page appears, in the win32 directory on the CD, double-click the issetup.exe file.
3. Select the language to use to run the installation wizard.
4. Follow the directions in the installation wizard to copy the required files to your computer.
5. In the **Finish** page of the installation wizard:
   - If you want to configure Cognos components immediately, click **Start Cognos Configuration**.
   - If you want to see late-breaking information about Cognos components, click **View the Readme**.
6. Click **Finish**.

   Use the Windows **Start** menu to start **Cognos Configuration** from the shortcut folder.

To ensure the security and integrity of Cognos 8, it is important to protect the installation directory from unauthorized or inappropriate access.

If you use Oracle or DB2 as the database server for the metric store in a distributed installation, you must now install the database client software (p. 127) on the same computer where you installed Metric Designer.

After you install Metric Designer on your Windows computer, some configuration tasks may be required to ensure that it works in your scorecarding environment (p. 188).

Default Settings for Metric Designer

The following table lists the default settings for the ports and URIs that are used by Metric Designer. After installation, you can use Cognos Configuration to change the settings. You can also change them by editing the cogstartup.xml file in the *c8_location*\configuration directory.

Component	Default	Description
Gateway	http://localhost:80/ cognos8/cgi-bin/ cognos.cgi	The URI to the gateway
Dispatcher URI for external applications	http://localhost:9300/ p2pd/servlet/dispatch	The URI to the dispatcher

Uninstalling Cognos 8

It is important to use uninstall programs to completely remove all files and modifications to system files.

To uninstall Cognos 8, you uninstall server components and modeling tools.

If you are running Cognos 8 in an application server environment, use the administration tool provided by your application server vendor to stop the application if it is running and undeploy the Java portion of Cognos 8 components. Many application servers do not completely remove all deployed application files or directories during an undeploy therefore you may have to perform this action manually. After you have undeployed Cognos 8 components, complete the steps in this chapter to uninstall on UNIX (p. 113) and on Windows (p. 114).

Uninstall Cognos 8 on UNIX or Linux

If you no longer require Cognos 8 or if you are upgrading, uninstall Cognos 8.

If you are upgrading from an older version of ReportNet to Cognos 8, follow the uninstallation instructions in the documentation for the older version of ReportNet.

Steps

1. If the console attached to your computer does not support a Java-based graphical user interface, determine the process identification (pid) of the Cognos 8 process by typing the following command:

   ps -ef grep cogbootstrapservice

2. Stop the Cognos 8 process:
   - If you run XWindows, start Cognos Configuration, and from the **Actions** menu, click **Stop**.
   - If you do not run XWindows, type:

     kill -TERM pid

3. To uninstall Cognos 8, go to the *c8_location*/uninstall directory and type the appropriate command:
   - If you use XWindows, type

     ./uninst -u

   - If you do not use XWindows, type

     ./uninstcc -u

4. Follow the prompts to complete the uninstallation.
5. Delete all temporary Internet files.

Uninstalling does not remove any files that changed since the installation, such as configuration and user data files. Your installation location remains on your computer, and you retain these files until you delete them manually.

Important:

- Do not delete the configuration and data files if you are upgrading to a new version of Cognos 8 and you want to use the configuration data with the new version.
- If you are using Cognos Content Database, the default location for the database files is in the *c8_location*/contentstore directory. If you want to keep your database after uninstalling, do not delete this directory.

Uninstall Cognos 8 on Windows

If you no longer require Cognos 8 or if you are upgrading, uninstall all Cognos 8 components and the Cognos 8 service.

If you installed more than one component in the same location, the uninstall wizard lets you choose the packages to uninstall. All components of the package will be uninstalled. You must repeat the uninstallation process on each computer that contains Cognos 8 components.

It is not necessary to back up the configuration and data files on Windows. These files are preserved during the uninstallation.

We recommend that you close all programs before you uninstall Cognos 8. Otherwise, some files may not be removed.

Uninstalling does not remove any files that changed since the installation, such as configuration and user data files. Your installation location remains on your computer, and you retain these files until you delete them using Windows Explorer.

Important: Do not delete the configuration and data files if you are upgrading to a new version of Cognos 8 and you want to use the configuration data with the new version.

Steps

1. From the **Start** menu, click **Programs**, **Cognos 8**, **Uninstall Cognos 8**.

   The **Uninstall** wizard appears.

   Tip: Cognos 8 is the default name of the Program Folder that is created during the installation. If you chose another name, go to that folder to find the program.

2. Follow the instructions to uninstall the components.

   The cognos_uninst_log.htm file records the activities that the Uninstall wizard performs while uninstalling files.

   Tip: To find the log file, look in the Temp directory.

3. Delete all temporary Internet files.

   For more information, see your Web browser documentation.

Uninstall Cognos Content Database

If you want to uninstall only Cognos Content Database and leave other Cognos 8 components on your computer, you must use the following procedure. After you uninstall Cognos Content Database you must configure a new content store before you can restart the Cognos 8 service.

If you installed only Cognos Content Database, use another procedure. For information about this procedure, see "Uninstall Cognos 8 on UNIX or Linux" (p. 113) or "Uninstall Cognos 8 on Windows" (p. 114).

Steps

1. On the computer where you installed Cognos Content Database, go to the *c8_location*\bin directory, and type the following command:

   - On Windows, type

     derby.bat uninstall

     This command removes the Cognos Content Database service.

   - On UNIX, type

     derby.sh stop

This command stops the Cognos Content Database service.

2. In the *c8_location* directory, delete the derby10.1.2.1 directory.
3. In the *c8_location*\bin directory, delete the following files:
   - On Windows, derby.bat
   - On UNIX, derby.sh and derbyenv.sh
4. On Windows, in the *c8_location*\logs directory, delete the derby.service file.
5. In the *c8_location* directory, open the cmplst.txt file in a text editor.
6. Remove lines containing Cognos Content Database values. The lines contain CCD and CMDERBY. For example:

   ```
   C8BISRVRCCD_version=

   C8BISRVRCCD_name=

   CCD_version=

   CCD_name=

   CMDERBY_version=

   CMDERBY_name=
   ```

   Tip: You can also comment the lines out by inserting # at the start of each line.
7. Save the file.
8. Start Cognos Configuration.
9. Under **Data Access**, **Content Manager**, do the following:
   - Delete the Cognos Content database.
   - Configure a new database resource to point to a new content store.

   For more information, see "Set Database Connection Properties for the Content Store" (p. 147).
10. Restart Cognos 8.

Chapter 7: Setting Up the Environment

After you install Cognos 8, you must set up resources in your environment so that the components can operate. For Cognos 8, you must create the database to be used as the content store. For Metric Studio, you must create at least one database to be used as a metric store. For Cognos 8 for reporting, you must create the data sources for Framework Manager.

You must ensure that a Java Runtime Environment (JRE) is available. You must ensure that a Web browser and a Web server are set up to provide access to Cognos components. If you use a router, you must configure it to support Cognos features.

Use the following checklist to guide you through the setup process:

- ❑ Create the database for the content store and, if using Metric Studio, a metric store.
- ❑ Set up the database client for the content store (Oracle, DB2 and Sybase) and, if using Metric Studio, a metric store (Oracle and DB2).
- ❑ Set up environment variables on UNIX for the metric store, if using Metric Studio.
- ❑ Update the Java environment, if required.
- ❑ Configure the Web server.
- ❑ Configure Web browsers.
- ❑ Configure a user account for Cognos 8
- ❑ Configure the router to test whether a dispatcher is available, if required.
- ❑ Set up the data source environment for Framework Manager, if required.
- ❑ Set up the database client for Framework Manager, if required.
- ❑ Set up the data source environment for Cognos 8 Transformer, if required.
- ❑ Set up the database client for Cognos 8 Transformer, if required.
- ❑ Set up import sources for Metric Designer, if required.
- ❑ Set up the database client for Metric Designer, if required.
- ❑ Set up ODBC connections to Sybase IQ or Netezza, if required.

After you complete these tasks, you must configure the Cognos components (p. 145) to work in your environment.

If you installed and want to use Cognos Content Database, you do not have to create a database or set up a database client. A database was created during the installation and Cognos 8 is already configured to use it. If you want to use another database as the content store, ensure that you set the correct database connection properties. For more information, see "Set Database Connection Properties for the Content Store" (p. 147).

Create the Content Store

The content store is a database that Content Manager uses to store global configuration data, global settings (such as the language and currency formats shown in the user interface), connections to data sources, and product-specific content. Design models and log files are not stored in the content store.

By default, Cognos 8 products share the content store database. You must create this database using one of the following:

- Microsoft SQL Server
- Oracle
- DB2
- Sybase Adaptive Server Enterprise (ASE)

On Linux, you can use Oracle, DB2, or Cognos Content Database for the content store.

A Microsoft SQL Server or Oracle database can use UTF-8 or UTF-16 encoding. A DB2 or Sybase database must use UTF-8 encoding. All database types must use the TCP/IP protocol, which is required by Cognos 8 to access data.

Note that Cognos 8 uses a single sort order that specifies the rules used by the database to interpret, collect, compare, and present character data. For example, a sort order defines whether the letter A is less than, equal to, or greater than the letter B; whether the collation is case sensitive; and whether the collation is accent sensitive. For more information about collation and collation sequences, see the database vendor documentation.

Your database administrator must back up Cognos 8 databases regularly because they contain the Cognos data. To ensure the security and integrity of databases, protect them from unauthorized or inappropriate access.

If you are upgrading from ReportNet, you can use your existing content store with Cognos 8. After the content store is upgraded to Cognos 8, you cannot use it with ReportNet. If you are upgrading and you want to keep the existing version of ReportNet, you must create a new content store database for use with Cognos 8. You must follow the appropriate upgrade process (p. 61) when creating the new content store database.

If you installed and are using Cognos Content Database as your content store, a database is already created and configured. However, you can create another database instance using Cognos Content Database.

Steps for Microsoft SQL Server

1. Ensure that your installation of Microsoft SQL Server is configured as follows:
   - UTF-8 or UTF-16 encoding is used

     For more information about character sets, encoding, and collation, see the Microsoft SQL documentation.
   - the collation sequence is case-insensitive

In a Custom installation, you choose a collation, which includes character sets and sort order, during the SQL Server setup. In a Typical installation, the installation uses the locale identified by the installation program for the collation. This setting cannot be changed later.

- the TCP/IP protocol is enabled

  This protocol is required by Cognos 8 to access data.

2. Open Microsoft SQL Server Management Studio and connect to the database server using SQL server authentication.

   If you connect using Windows authentication, the database that you create will also use Windows authentication. Cognos 8 is configured by default to use a database with SQL server authentication.

3. Create the database.

   If you connected to the database server using Windows authentication, you must configure the database connection using a database type of **SQL Server database (Windows Authentication)** in Cognos Configuration.

   For more information, see "Set Database Connection Properties for the Content Store" (p. 147).

4. Create the user account that will be used to access the database:
   - Under **Security**, right click **Logins** and select **New Login**.
   - Specify a Login name.
   - Select **SQL Server authentication** and specify the **Password**.
   - Clear **Enforce password policy**.

     This clears all three check boxes.

   - Click **OK**.

   Tip: If you want to host more than one content store on your Microsoft SQL Server instance and you will use both at the same time, use a different user account for each content store to ensure that each Cognos 8 instance is fully isolated from the others.

5. Create a schema:
   - Under **Databases**, expand the database (***new_database***) that you created in step 3.
   - Under ***new_database***, expand **Security**.
   - Right-click **Schemas** and select **New Schema**.
   - Specify the **Schema name** and click **OK**.

6. Configure the database user:
   - Under **Databases**, ***new_database***, **Security**, right click **Users** and select **New User**.
   - Specify the **User name**.

- For **Login name**, browse and select the login that you created in step 4.
- For **Default schema**, browse and select the schema that you created in step 5.
- In the **Owned Schemas** list, select the same schema as **Default schema**.
- In the **Role Members** list, select **db_datareader**, **db_datawriter**, and **db_ddladmin**.
- Click **OK**.

7. Repeat steps 4 to 6 for each new user account.

Steps for Oracle

1. Ensure that the parameter for the database instance compatibility level of the content store database is set to 9.0.1 or higher.

   For information about changing an instance configuration parameter, see the Oracle documentation.

2. Determine if the database is Unicode.

   Tip: One method is to type the following select statement:

   select * from NLS_DATABASE_PARAMETERS

   The result set returns NLS_CHARACTERSET as UTF-8 or UTF-16, or AL32UTF8 or AL16UTF16, or not Unicode.

   If the result set returns an NLS_CHARACTERSET that is not Unicode, create a new database and specify AL32UTF8 or UTF-8 for the database character set parameters.

3. Determine which user account will be used to access the database.

   Tip: If you want to host more than one content store on your Oracle instance and you will use both at the same time, use a different user account for each content store to ensure that each Cognos 8 instance is fully isolated from the others.

4. Ensure that the user account that accesses the database has permission to do the following:
   - connect to the database
   - create, alter, and drop tables, triggers, views, procedures, and sequences
   - insert, update, and delete data in the database tables

Steps for DB2

1. Set the appropriate environment variables for DB2.

Environment variable	Description
DB2DIR	The top level directory that contains the database client software or the entire database installation.
*library*PATH	The load library path.You must add driver location. Examples:
On Solaris: LD_LIBRARY_PATH	Solaris example: LD_LIBRARY_PATH= $DB2DIR/lib: $LD_LIBRARY_PATH
On AIX: LIBPATH	AIX example: LIBPATH=$DB2DIR/lib: $LIBPATH
On HP-UX: SHLIB_PATH	HP-UX example: SHLIB_PATH=$DB2DIR/lib: $SHLIB_PATH
DB2INSTANCE	The default database server connection.
DB2CODEPAGE	Setting this optional environment variable to a value of 1208 provides support for multilingual databases. For information about whether to use this environment variable, see the DB2 documentation.

2. Determine if the database is Unicode by typing the following at the command prompt:

   db2 get database configuration for database_name

   The codepage is Unicode if it has a value of 1208.

3. If the codepage is not Unicode, create a new database that has a codepage value of 1208.

4. Ensure that you set the following configuration parameters.

Property	Setting
Application heap size (applheapsz)	1024k
Lock timeout	4 min. (or 240 sec.) Do not set this to an infinite timeout value.

5. Create a buffer pool with a page size of 32k.
6. Create a system temporary tablespace with a page size of 32k.
7. Create a user temporary tablespace with a page size of 4k.

   Global temporary tables will be created in the user temporary tablespace.
8. Create a regular user tablespace with a page size of 4k.
9. If you already created the content store and are now creating a logging database, create an additional regular user tablespace with a page size of 8k.
10. Determine which user account Cognos 8 will use to access the database.

    Tip: If you want to host more than one content store on your DB2 instance and you will use both at the same time, use a different user account for each content store to ensure that each Cognos 8 instance is fully isolated from the others.
11. Grant create and drop table privileges on the database to the user account.

    Ensure that the user account has CREATETAB, CONNECT and IMPLICITSCHEMA privileges for the database.

    Ensure that the user account has USE privileges for the USER TEMPORARY tablespace and other appropriate tablespaces associated with the database.

    For Windows XP, ensure that the user account has GRANT privileges for the USER TEMPORARY tablespace.

Steps for Sybase Adaptive Server Enterprise

1. On the Sybase server, create a server instance with an 8K server page size.

   For instructions, see the Sybase documentation.
2. If required, install jConnect 5.5.

   This tool sets up the communication between the JDBC driver and the Sybase Adaptive Server instance.

   For instructions, see the Sybase documentation.

   If your version of Sybase does not include JConnect 5.5, you must download the installer from Sybase's Web site.

3. Add the UTF-8 character set to the server instance.
4. If required, make UTF-8 the default character set on the server.
5. Create a database device.

   Tip: Set **log_segment** to a minimum of 10 MB.
6. Set the new database device as the default.

   Information about the new database will be stored in the new database device. Keep a backup of the database device for recovery purposes.
7. Create the database.
8. Determine which user account will be used to access the database.

   Tip: If you want to host more than one content store on your Sybase instance and you will use them at the same time, use a different user account for each content store to ensure that each Cognos 8 instance is fully isolated from the others.
9. Grant create and drop table privileges on the database to the user account.

   Ensure that the user account has the following privileges for the database: create default, create procedure, create rule, create table, and create view.
10. For the database, set the **Select into** property to True and restart the server.

Steps for Cognos Content Database

1. On the computer where you installed Cognos Content Database, go to the *c8_location*\derby10.1.2.1\bin directory.

   You need only to perform this task if you want to create another content store database in Cognos Content Database. During Cognos Content Database installation, a database was created and Cognos 8 is already configured to use that database.
2. Start the ij utility using the ij.bat or ij.ksh script.

   The ij utility is a command line utility for creating and managing Cognos Content Database.
3. Create a database by typing the following ij utility command:

   connect 'jdbc:derby://*host*:*port*/*db_name*;create=true;user=*username*; password=*password*';

   For example, to create a database named contentstore on the localhost computer on port number 1527 as a user named cognos with a password of cognos, you would type

   connect 'jdbc:derby://localhost:1527/contenstore;create=true;user=cognos;password=cognos';

   The database name is case sensitive.

   The database files are located in the *c8_location*\contentstore directory.
4. Close the ij utility by typing the following command:

   disconnect;

Create the Metric Store

A metric store is a database that contains content for metric packages. A metric store also contains scorecarding application settings, such as user preferences. You must create a metric store database using Oracle, Microsoft SQL Server, or DB2.

If you installed Cognos Content Database, it cannot be used as a metric store database.

Your database administrator must back up Cognos 8 databases regularly because they contain the Cognos data. To ensure the security and integrity of databases, it is also important to protect them from unauthorized or inappropriate access.

Steps for Microsoft SQL Server

1. In the *c8_location*/configuration/schemas/cmm/sqlserver directory, run the cmm_create_db.cmd script by typing the following command:

   path_to_script **cmm_create_db** ***host_namedatabase_nameuser_namepassword*** **[*user_to_create*]**

   Use the following values in your command.

Value	Setting
host_name	The name of the computer where the database will be created.
database_name	The name of the database that will be created.
user_name	The user ID with permissions to create the database. The user ID must have permission to create the database, such as the sa user.
password	The password for the *username*.
user_to_create	The user created by the script and given database owner permissions. This value is optional.

2. Determine which user account Metric Studio will use to access the database.

   The user account must be the database owner (dbo) or aliased to the database owner.

Steps for Oracle If the Database Does Not Exist

1. Ensure that you are logged into the Oracle server as a user that is a member of the ORA_DBA user group on Windows or the dba group on UNIX.
2. Set the NLS_LANG (National Language Support) environment variable to the UTF-8 character set on the metric store computer by typing the following command:

NLS_LANG = language_territory.character_set

Examples are:

- NLS_LANG = AMERICAN_AMERICA.UTF8
- NLS_LANG = JAPANESE_JAPAN.UTF8

The value of the variable determines the locale-dependent behavior of Cognos 8. Error messages, sort order, date, time, monetary, numeric, and calendar conventions automatically adapt to the native language and locale.

3. From the *c8_location*/configuration/schemas/cmm/oracle directory, run the cmm_create_db.cmd script by typing the following command:

   path_to_script **cmm_create_db** ***sidpathdatabase_version*** [***user_to_create***]

   Use the following values in your command.

Value	Setting
path_to_script	The path to the script. For example, *c8_location*/configuration/schemas/cmm/oracle/
sid	The SID for the new database that will be created.
path	The path where the data files will be created.
database_version	The version of Oracle software that is installed. For example, oracle9 or oracle10.
user_to_create	The user created by the script and given database owner permissions. This value is optional.

4. Determine which user account Metric Studio will use to access the database.

   If you included the optional user in the previous step, this is the user you will use to access the database. If you did not include a user, then you must use a valid Oracle database username with the following permissions granted:

   - CREATE TABLE, CREATE VIEW, CREATE PROCEDURE, CREATE TRIGGER, CREATE TYPE, CREATE SEQUENCE, and CREATE SESSION
   - EXECUTE on DBMS_LOCK and DBMS_UTILITY packages.

The CREATE TABLE and CREATE TRIGGER permissions must be granted directly to the user account rather than to a role.

Steps for Oracle If the Database Exists

1. Ensure that you are logged into the Oracle server as a user that is a member of the ORA_DBA user group on Windows or the dba group on UNIX.
2. Set the NLS_LANG (National Language Support) environment variable to the UTF-8 character set on the metric store computer by typing the following command:

   NLS_LANG = language_territory.character_set

   Examples are:

   - NLS_LANG = AMERICAN_AMERICA.UTF8
   - NLS_LANG = JAPANESE_JAPAN.UTF8

   The value of the variable determines the locale-dependent behavior of Cognos 8. Error messages, sort order, date, time, monetary, numeric, and calendar conventions automatically adapt to the native language and locale.
3. Determine which user account Metric Studio will use to access the database. You must use a valid Oracle database username with the following permissions granted:

   - CREATE TABLE, CREATE VIEW, CREATE PROCEDURE, CREATE TRIGGER, CREATE TYPE, CREATE SEQUENCE, and CREATE SESSION
   - EXECUTE on DBMS_LOCK and DBMS_UTILITY packages.

   The CREATE TABLE and CREATE TRIGGER permissions must be granted directly to the user account rather than to a role.

Steps for DB2

1. In the *c8_location*/configuration/schemas/cmm/db2 directory, run the cmm_create_db.cmd script by typing the following command:

   On Windows, type

   cmm_create_db ***dbinstanceuser_namepassworddbname drivedbalias***

   On UNIX, type

   cmm_create_db.sh ***dbinstanceuser_namepassworddbname drivedbalias***

   Use the following values in your command.

Value	Setting
dbinstance	The DB2 instance name where the database will be created.

Value	Setting
user_name	The user ID with permissions to create the database. The user ID must have SYSADM or SYSCTRL privileges, and must have DBADM privileges to create the schema.
password	The password for the *username*.
dbname	The name of the database that will be created. The name must have a maximum of 8 characters, and it cannot start with a number.
drive/path	On Windows, the drive on which the database objects will be created. On UNIX, the path where the database objects will be created.
dbalias	The database alias name. This value is optional.

Note: Your database administrator can review the scripts to ensure they suit your environment. The initializedb.db2 script is invoked by the cmm_create_db.cmd script and defines the buffer pools and tablespaces.

2. Determine which user account Metric Studio will use to access the database.

   The user account must have DBADM privileges.

   Note: If your DB2 server is an earlier version than 8.2, and compiles stored procedures using a platform-specific, third party C compiler, the compiler must be installed on each DB2 server computer used to the metric store.

Set Up the Database Client

If you use Oracle, DB2, or Sybase as the database server for the content store, additional steps are required after you install Cognos 8 before you can configure it. You must set up the database client on every computer where Content Manager, Framework Manager, or Cognos 8 Transformer is installed. The database client supports the use of Cognos 8 packages and reports, as data sources, in Framework Manager and Cognos 8 Transformer. To set up the database client, perform the following steps.

Database	Additional Steps
Oracle	Set up the JDBC driver.

Database	Additional Steps
DB2	Set up the database client software and the JDBC 2.0 driver. On UNIX, ensure that the 32-bit DB2 libraries are in the library search path, which is usually the $DB2DIR/lib directory or the $DB2DIR/lib32 directory.
Sybase	Set up the JDBC driver.
Microsoft SQL Server	No additional steps are required. The JSQLConnect.jar is installed to the appropriate location by default.
Cognos Content Database	No additional steps are required.

If you use Oracle or DB2 for metric stores, you must set up the following on every computer where Application Tier Components for Metric Studio or Metric Designer are installed.

Database	Additional Steps
Oracle	Set up the JDBC OCI driver. Install the SQL Loader utility.
DB2	Set up the database client software and the JDBC 2.0 driver.
Microsoft SQL Server	The JSQLConnect.jar is installed to the appropriate location by default. You must install the bcp utility.

If you use Oracle for your metric store, you must install the SQL Loader utility on every computer where Application Tier Components for Metric Studio or Metric Designer are installed.

If you use Microsoft SQL Server, you must install the bcp utility on every computer where Application Tier Components for Metric Studio or Metric Designer are installed.

Steps for Oracle

1. On the computer where the Oracle client is installed, go to the ORACLE_HOME/jdbc/lib directory.

2. Copy the ojdbc14.jar file to the *c8_location*/webapps/p2pd/WEB-INF/lib directory on computers where Content Manager is installed.

   If the directory contains the classes12.jar file, delete it before installing the ojdbc14.jar file.

   If you are using Metric Studio, copy the ojdbc14.jar file to the *c8_location*/webapps/p2pd/WEB-INF/lib directory on computers where Metric Studio is installed.

   This file includes the driver required by the content store.

Steps for DB2

1. Install the DB2 client software on the appropriate computers.
2. If the content store is on a different computer from Content Manager, configure a database alias to the content store by running the DB2 Client Configuration Assistant.

   On UNIX or Linux, use the DB2 command line interface.

   If the content store database and Content Manager are on the same computer, the content store name automatically becomes the alias.

   When you configure the Content Manager computers, ensure that they are all configured to use the same content store.
3. On Windows, stop the DB2 services and the HTML Search Server.
4. To copy the JDBC2 driver, copy the *DB2_installation*/sqllib/java/db2java.zip file to the *c8_location*/webapps/p2pd/WEB-INF/lib directory.
5. Rename the db2java.zip file to db2java.jar.
6. On Windows, restart the DB2 services and the HTML Search Server.
7. Repeat this entire procedure on the Cognos 8 computers where the software must be installed.

You can tune the database to take advantage of DB2 features. For more information, see the *Architecture and Deployment Guide*.

Steps for Sybase

1. On the computer where Sybase is installed, go to the Sybase_location/jConnect-5_5/classes directory.
2. Copy the jconn2.jar file to the *c8_location*/webapps/p2pd/WEB-INF/lib directory on every computer where Content Manager is installed.

If the installation is complete, some configuration tasks are required to ensure that Cognos 8 (p. 145) and Framework Manager (p. 176) work in your environment.

For information about configuring Metric Designer, see "Configure Metric Designer" (p. 188).

Setting Up Environment Variables on UNIX for the Metric Store

For Cognos 8, you must specify environment variables before you can use a DB2 or Oracle database as the metric store.

The proper syntax for creating environment variables is shell dependent.

Oracle

For Oracle databases, you must set and export the database environment variables for the user of the metric store before you start the Cognos processes. Cognos 8 uses these database variables to connect to your database. One way to set these environment variables is to include these commands in the .profile or .login script of the user who starts the Cognos services.

When you set the load library paths, ensure that the 32-bit Oracle libraries are in the library search path, which is usually the $ORACLE_HOME/lib directory or the $ORACLE_HOME/lib32 directory if you installed a 64-bit Oracle client.

The following table describes environment variables for Oracle databases. Contact your database or network administrator for the correct values for your system.

Environment variable	Description
ORACLE_HOME	The top level directory that contains the database client software or the entire database installation. Example: /usr/oracle You may be able to use an Oracle script to create the environment variables. For more information, see the Oracle documentation. Example: /usr/local/bin/coraenv
TNS_ADMIN	The directory that contains the Oracle tnsnames.ora file, which allows calls to the Oracle database to determine the required server connections. Example: $ORACLE_HOME/network/admin
PATH	The variable to locate executable files. Example: $PATH:$ORACLE_HOME/bin
*library*PATH	The load library path.

Environment variable	Description
On Solaris:	Solaris Examples:
LD_LIBRARY_PATH	LD_LIBRARY_PATH=$ORACLE_HOME/ lib:$LD_LIBRARY_PATH LD_LIBRARY_PATH=$ORACLE_HOME/ lib32:$LD_LIBRARY_PATH
On AIX:	AIX Examples:
LIBPATH	LIBPATH=$ORACLE_HOME/ lib:$LIBPATH LIBPATH=$ORACLE_HOME/ lib32:$LIBPATH
On HP-UX:	HP-UX Examples:
SHLIB_PATH	SHLIB_PATH=$ORACLE_HOME/ lib:$SHLIB_PATH SHLIB_PATH=$ORACLE_HOME/ lib32:$SHLIB_PATH
NLS_LANG	The value of the variable determines the locale-dependent behavior of Cognos 8. Error messages, sort order, date, time, monetary, numeric, and calendar conventions automatically adapt to the native language and locale.

DB2

For IBM DB2 databases, you must set the database variables by running the environment setup scripts included with the IBM DB2 installation. For Bourne or Korn shells, run the following command or add it to the .profile script:

DB2_installation_path/db2profile

Contact your database or network administrator for the correct values for your system.

Update the Java Environment

Cognos 8 cryptographic services use a specific .jar (Java Archive) file, named bcprov-jdk*nn-nnn*.jar, that must be located in your Java Runtime Environment (JRE). This file provides additional encryption and decryption routines that are not supplied as part of a default JVM installation. To ensure security, the encryption file must be loaded by the JVM using the java extensions directory.

If you want to use your own JRE and have JAVA_HOME set to that location on Windows or if you are installing on UNIX, you may have to update the Java environment for the cryptographic services.

On Windows, you can set JAVA_HOME as a system variable or a user variable. If you set it as a system variable, it may be necessary to restart your computer for it to take effect. If you set it as a user variable, set it so that the environment in which Tomcat is running can access it.

If you do not have a JAVA_HOME variable already set on Windows or if JAVA_HOME points to a Java version that is not valid for Cognos 8, the JRE files provided with the installation will be used, and you do not have to update any files in your environment.

Steps

1. Ensure that the JAVA_HOME environment variable is set to the JRE location.

   For example, to set JAVA_HOME to the JRE files provided with the installation, the path is *c8_location*/bin/jre/*version*.

2. Copy the bcprov-jdk*nn-nnn*.jar file from the *c8_location*/bin/jre/*version*/lib/ext directory to the *Java_location*/jre/lib/ext directory.

Configure the Web Server

For all installations, before you use Web pages generated by Cognos 8, you must configure your Web server. You must set up virtual directories, also known as Web aliases, for the directories that contain the HTML and Web files for Cognos 8. For Cognos 8 for reporting, you must also set the content expiry for the images directory in your Web server so that the Web browser does not check image status after the first access.

You must set up virtual directories, also known as Web aliases, for your Cognos 8 environment. The virtual directories must be created to connect to the Cognos 8 portal and for client applications to be able to connect to the server.

On UNIX and Linux, the account under which the Web server runs must have read access to the cogstartup.xml file in the *c8_location*/configuration directory. By default the cogstartup.xml file has read permission for others. If you run your Web server under a specific group, you can change the cogstartup.xml file permissions to ensure that it belongs to the same group as the Web server. You can then remove the read permission for others.

Steps

1. Create the following virtual directories:

Alias	Location	Permission
cognos8	*c8_location*/webcontent	Read
cognos8/cgi-bin	*c8_location*/cgi-bin	Execute

   You can use a name other than cognos8 in the aliases. However, you must use cgi-bin as the second part of the alias and you must change the virtual directory in the **Gateway URI** property to match the new Cognos alias. For more information, see "Change a URI" (p. 196).

If you are upgrading from ReportNet, you can continue to use the existing aliases. If you install Cognos 8 reporting components in a different location from ReportNet, change the existing aliases to include the new location. If you have more than one version of ReportNet on one computer, you must use different alias names for Cognos 8.

For Apache Web Server, ensure that you define the cognos8/cgi-bin alias before the cognos8 alias in the httpd.conf file located in the *Apache_installation*/conf directory. The cognos8/cgi-bin alias must be defined as a ScriptAlias.

2. If you want to use Report Studio's image browser, enable Web Distributed Authoring and Versioning (WebDAV) on your Web server.

   If you use Apache Web Server, specify a directory in which to enable WebDAV. For information about configuring WebDAV, see your Web server documentation.

3. For Cognos 8 for reporting, set the content expiry on the *c8_location*/pat/images virtual directory in your Web server.

   Each time a user opens Report Studio, their Web browser checks with the Web server to determine if images are current. Because there are over 600 images, this can result in excess network traffic. You can postpone this check until a specified date by using the content expiry feature of the Web server.

   For information on setting content expiry, see the documentation for your Web server.

   Note: When you upgrade, Report Studio users must clear their Web browser cache to get the latest images.

If you use Web aliases other than cognos8, or your Web server is on another computer, or you are using Microsoft Internet Application Interface (ISAPI), apache_mod or a servlet gateway, change the Gateway URI (p. 231) when you configure Cognos components.

Enable SSL on the Web Server

Enable secure sockets layer (SSL) to encrypt a user's communication with the Web server.

To enable SSL on your Web server, you must obtain a Web server certificate signed by a Certificate Authority and install it into your Web server. The certificate must not be self-signed, because self-signed certificates will not be trusted by Cognos components.

To enable Cognos components to use an SSL-enabled Web server, you must have copies of the trusted root certificate (the certificate of the root Certificate Authority which signed the Web server certificate) and all other certificates which make up the chain of trust for the Web server's certificate. These certificates must be in Base64 encoded in ASCII (PEM) or DER format, and must not be self-signed. The certificates must be installed on every computer where you have installed Application Tier Components.

For more information about installing certificates into your Web server, see your Web server documentation.

Steps

1. Configure the Web server for SSL and start the Web server.

For more information, see your Web server documentation

2. On each Application Tier Components computer that points to the gateway on the Web server, in Cognos Configuration, change the gateway URI from HTTP to HTTPS, and save the configuration.

   Important: Do not start the Cognos 8 service yet.

3. On each Planning Server computer that points to the gateway, in Cognos Configuration, change the gateway URI from HTTP to HTTPS, and save the configuration.

   Important: Do not start the Cognos 8 service yet.

4. On each Application Tier Components computer, go to the *c8_location*/bin directory and import all of the certificates that make up the chain of trust, in order starting with the root CA certificate, into the Cognos trust store.

   Import the certificates by typing the following command:

   On UNIX or LINUX, type

   ThirdPartyCertificateTool.sh -T -i -r *certificate_fileName* -D ../configuration/signkeypair -p *password*

   On Windows, type

   ThirdPartyCertificateTool.bat -T -i -r *certificate_fileName* -D ../configuration/signkeypair -p *password*

   Note: The password should have already been set. If not, the default password is NoPassWordSet.

5. On each Planning Server computer, go to the *c8_location*/bin directory and import all of the certificates that make up the chain of trust, in order starting with the root CA certificate, into the Cognos trust store.

   Import the certificates by typing the following command:

   ThirdPartyCertificateTool.bat -T -i -r *certificate_fileName* -D ../configuration/signkeypair -p *password*

   Note: The password should have already been set. If not, the default password is NoPassWordSet.

6. On each Application Tier Components computer, in Cognos Configuration, start the Cognos 8 service.

7. On each Planning Server computer, in Cognos Configuration, start the Cognos 8 service.

You can verify trust, by creating and running a PDF report that contains pictures that are not stored locally but which the gateway gets from a remote computer. If the pictures appear, trust is established.

To avoid being prompted by a security alert for each new session, install the certificate into one of your Web browser's certificate stores.

In addition, you may want to set up SSL connections between Cognos components and other servers. You must ensure that SSL is set up for the other servers and then you must set up a shared trust

between Cognos components and the other servers. For more information, see "Configuring the SSL Protocol" (p. 211).

Configure Web Browsers

Cognos 8 uses the default browser configurations provided by Microsoft, Netscape, and Firefox. For all browsers, you must ensure that settings are enabled for cookies and Java scripts. Additional required settings are specific to the browser.

The following table shows the settings that must be enabled in the supported Web browsers.

Browser	Setting	Cognos component
Internet Explorer (settings for studios and portals)	Allow Cookies Active Scripting Allow META REFRESH	Cognos Connection Cognos Administration Cognos Viewer Report Studio Query Studio Analysis Studio Event Studio Metric Studio
Internet Explorer (settings for some studios)	Run ActiveX controls and plug-ins Script ActiveX controls marked safe for scripting	Report Studio Query Studio Analysis Studio
Internet Explorer (settings for a single studio)	Binary and Script Behaviours Allow programmatic clipboard access	Report Studio
Netscape	Allow Cookies JavaScript	Cognos Connection Cognos Administration Query Studio Event Studio Metric Studio

Browser	Setting	Cognos component
Firefox	Allow Cookies Enable Java Enable JavaScript Load Images	Cognos Connection Cognos Administration Cognos Viewer Query Studio

Note: Report Studio and Query Studio use the native Microsoft Internet Explorer XML support, which is a component of the browser. ActiveX support must be enabled because Microsoft implements XML using ActiveX. Cognos 8 does not provide or download ActiveX controls. Only the ActiveX controls that are installed as part of Internet Explorer are enabled through this configuration.

Important: If Adblock Plus is installed with Firefox, disable it using the per-page option. Adblock Plus prevents some Cognos Connection resources from working properly.

Cognos 8 uses the following cookies to store user information.

Cookie	Type	Purpose
AS_TICKET	Session temporary	Created if Cognos 8 is configured to use a Cognos Series 7 namespace
caf	Session temporary	Contains security state information
Cam_passport	Session temporary	Stores a reference to a user session stored on the Content Manager server
cc_session	Session temporary	Holds session information that is specific to Cognos Connection
cc_state	Session temporary	Holds information during edit operations, such as cut, copy, and paste

Cookie	Type	Purpose
CRN	Session temporary	Contains the content and product locale information, and is set for all Cognos users
CRN_RS	Persistent	Stores the choice that the user makes for "view members folder" in Report Studio
PAT_CURRENT_FOLDER	Persistent	Stores the current folder path if local file access is used, and is updated after the Open or Save dialog box is used
qs	Persistent	Stores the settings that the user makes for user interface elements such as menus and toolbars
usersessionid	Session temporary	Contains a unique user session identifier, valid for the duration of the browser session.

After upgrading or installing new software, restart the Web browser and advise users to clear their browser cache.

Configure a User Account for Cognos 8

The account under which Cognos 8 runs must:

- have access to all required resources, such as printers and Web servers
- have the rights to logon as a service and act as part of the operating system
- be a member of the local admin group

For example, to print reports using a network printer, the account must have access to the network printer, or you must assign a logon account to the Cognos 8 service.

For Windows, we recommend that you assign a logon account to the Cognos 8 service. You can configure the Cognos 8 service to use a special user account by selecting the Cognos 8 service from the list of services shown in the Services window in Windows. You can then define the user account properties.

For UNIX or Linux, we recommend that you create a new UNIX or Linux group named cognos8. This group must contain the user that owns the Cognos files. Change the group ownership of the Cognos files to the cognos8 group and change the file permissions for all Cognos files to GROUP READABLE/WRITABLE/EXECUTABLE.

Configure the Router to Test Dispatcher Availability

If you use a router to distribute requests to Cognos 8 dispatchers, and the router can test the availability of a server using a test URL, you can configure the router to test the availability of a Cognos 8 dispatcher.

To test the availability of a dispatcher, do the following:

- Configure the router to use a URL with the path /p2pd/servlet/ping.

If the dispatcher is not ready, the following response is returned:

503 Service Unavailable

If the dispatcher is ready, the following response is returned:

200 OK

Set Up the Data Source or Import Source Environment

The Cognos 8 modeling tools create and manage metadata. Framework Manager creates and manages metadata for the reporting functions, Cognos 8 Transformer creates and manages metadata for PowerCubes, and Metric Designer creates and manages metadata required for the scorecarding functions. Because metadata is derived from data sources in multi-platform or multilingual environments, there are several things you must think about or do when you set up the data source environment for Framework Manager or Cognos 8 Transformer or set up the import source environment for Metric Designer. Commonly, these things depend on the third-party technology you use for your data or import source.

If you use a Sybase data source, these steps are not necessary.

If you upgraded from an older version of Framework Manager, you are not required to set up anything in the data source environment. You must set up the data source environment only if you installed Framework Manager in a different location from the older version.

Ensure that you install the appropriate language packs to support the character sets and currency symbols you use. For information about installing language packs, see the Cognos Supplementary Languages *Installation and Configuration Guide*.

If users operating in different languages will be connecting to a Microsoft Analysis Services (MSAS) data source, you must create a separate Cognos 8 instance for each language.

Steps

1. Set the environment variable for multilingual support:
   - For Oracle, set the NLS_LANG (National Language Support) environment variable on each computer where Framework Manager or Metric Designer and the Cognos 8 server are installed by typing the following command:

     NLS_LANG = language_territory.character_set

     Examples are:

     NLS_LANG = AMERICAN_AMERICA.UTF8

     NLS_LANG = JAPANESE_JAPAN.UTF8

     The value of the variable determines the locale-dependent behavior of Cognos 8. Error messages, sort order, date, time, monetary, numeric, and calendar conventions automatically adapt to the native language and locale.
   - For DB2, set the DB2CODEPAGE environment variable to a value of 1252.

     For more information about whether to use this optional environment variable, see the DB2 documentation.

   No settings are required for SAP BW. SAP support only a single code page on non-Unicode SAP BW systems.
2. For Oracle, add $ORACLE_HOME/lib to your LD_LIBRARY_PATH.

   When you set the load library paths, ensure that the 32-bit Oracle libraries are in the library search path, which is usually the $ORACLE_HOME/lib directory or the $ORACLE_HOME/lib32 directory if you installed a 64-bit Oracle client.
3. For Oracle, copy the ojdbc14.jar file from ORACLE_HOME/jdbc/lib to the *c8_location*/webapps/p2pd/WEB-INF/lib directory.

   If the directory contains the classes12.jar file, delete it before installing the ojdbc14.jar file.
4. For SAP BW, configure the following authorization objects so that the modeling tool can retrieve metadata.

   Some of the values shown, such as *, are default values that you may want to modify for your environment.

Authorization object	Field	Value
S_RFC	Activity	16

Authorization object	Field	Value
	Name of RFC to be protected	SYST, RSOB, SUGU, RFC1, RS_UNIFICATION, RSAB, SDTX, SU_USER
	Type of RFC object to be protected	FUGR
S_TABU_DIS	Activity	03
	Authorization Group	&NC&
S_RFC	Activity	16
	Name of RFC to be protected	SYST, RSOB, SUGU, RFC1, RS_UNIFICATION, RSAB, SDTX, SU_USER
	Type of RFC object to be protected	FUGR
S_TABU_DIS	Activity	03
	Authorization Groups	&NC&
S_USER_GRP	Activity	03, 05
	User group in user master main	*
S_RS_COMP	Activity	*
	Info Area	*InfoArea Technical Name*
	Info Cube	*InfoCube Technical Name*

Authorization object	Field	Value
	Name (ID) of reporting components	*
	Type of reporting components	*
S_RS_COMP1	Activity	*
	Name (ID) of reporting components	*
	Type of reporting components	*
	Owner (Person Responsible)	*
S_RS_HIER	Activity	71
	Hierarchy Name	*Hierarchy Name*
	InfoObject	*InfoObject Technical Name*
	Version	*Hierarchy Version*
S_RS_ICUBE	Activity	03
	InfoCube sub-object	DATA DEFINITION
	Info Area	*InfoArea Technical Name*
	InfoCube	*InfoCube Technical Name*

&NC& represents any table that does not have an authorization group. For security reasons, create a new authorization group and assign the table RSHIEDIR to it. The new authorization group restricts the user's access to the above table only, which is needed by the modeling tool. Create the new authorization group as a customization in the SAP system.

For more information about SAP BW authorization objects, see Transaction SU03.

After you complete these tasks, you must configure the Cognos 8 components (p. 145) to work in your environment.

Setting Up ODBC Connections to Sybase IQ or Netezza

If you are using an ODBC driver on UNIX or Linux to connect to a Sybase IQ or Netezza ODBC data source, you must configure the environment and define the data sources.

After setting up the ODBC connections, you must create connections to the data sources in Cognos Connection. For information, see the Cognos 8 *Administration and Security Guide*.

For UNIX, the open source iODBC driver manager provides ODBC connectivity to Sybase IQ or Netezza ODBC data sources. Cognos provides the binaries for this driver manager, which are automatically installed with Cognos 8.

On Linux, the unixODBC package provided with the operating system provides ODBC connectivity to Sybase IQ or Netezza ODBC data sources.

Steps

1. Verify that the ODBC connectivity software is properly installed:
   - On UNIX, verify that the binaries provided by Cognos for the iODBC installation are properly installed by typing the following at the command prompt:

     which iodbctest *c8_location*/bin/iodbctest
   - On Linux, verify that the unixODBC package provided with the operating system is properly installed by typing the following at the command prompt:

     odbcinst -version unixODBC *version*

     If problems occur when using this command, see the documentation provided by your Linux vendor.
2. Set the appropriate library path environment variable to specify the location of the ODBC libraries for your operating system.
   - For Linux, ensure that the variable specifies the /usr/lib directory that contains libodbc.so before any other database installation directories.
   - For UNIX, ensure that the variable includes the *c8_location*/bin directory before any other database installation directories.

   This table lists the environment variables for each operating system that must specify the location of the ODBC libraries.

Operating system	Environment variable
AIX	LIBPATH
Solaris and Linux	LD_LIBRARY_PATH

Operating system	Environment variable
HP-UX	SHLIB_PATH

3. Copy the *ODBC_location*/lib/odbc.ini file to *c8_location*/bin.
4. Rename the odbc.ini file located in the *c8_location*/bin directory to **.odbc.ini**
5. In the [ODBC] section, specify the ODBC root directory and whether Driver Manager tracing is enabled.

   Here is an example:

   ```
   [ODBC]
    InstallDir=/isvdb/sql/odbc
    Trace =1
    TraceFile = /uda/dev/boileaum/trace.log
    TraceAutoStop=1
   ```

6. In the [ODBC Data Sources] section, define the name and driver for each data source.

   Here is an example:

   ```
   [ODBC Data Sources]dsn-name=
   driver-description
   ```

7. Create a copy of the [dsn-name] section for each data source defined in the [ODBC Data Sources] section.
8. For each data source defined in the [ODBC Data Sources] section, define additional details using a [dsn-name] section.

   Here is an example:

   ```
   [dsn-name]
    Driver=driver_path Keyword=value
   ```

9. If you want to define a data source that is used when no other data source is available, create a [Default] section, as shown here:

   ```
   [Default]
    Driver=driver-path Keyword=value
   ```

10. Save and close the odbc.ini file.
11. Test the connection to the data source by doing one of the following:
    - On UNIX, type the following command at a command prompt and then run a Select from a known table:

      iodbctest DSN=*dns-name*;UID=*userID*;PWD=*password*

    - On Linux, test the connection using the odbctest application.

Chapter 8: Configuring Cognos 8

After you install one or more Cognos 8 components on your computer, you must configure them to work in your Cognos environment. Initially, default property settings chosen by Cognos are used to configure the components. However, you may want to change these default settings if existing conditions make the default choices inappropriate, or to better suit your environment.

For all Windows and most UNIX and Linux installations, use Cognos Configuration to configure your settings. However, if the console attached to the UNIX or Linux computer on which you are installing Cognos 8 components does not support a Java-based graphical user interface you must manually edit the cogstartup.xml file in the *c8_location*\configuration directory, and then run Cognos Configuration in silent mode.

For all types of installations (p. 27), some configuration tasks are required. For example, you must configure your Web server and specify the database connection properties to the content store.

If you distribute Cognos 8 across several computers, some additional configuration tasks are required to ensure that the components can communicate with each other. The order in which you configure and start the components is also important.

Other configuration tasks are optional and depend on your Cognos environment. Use these optional configuration tasks to customize your configuration so that Cognos 8 easily integrates into your existing environment. For example, you can configure features for Cognos Application Firewall or specify the amount of resources Cognos 8 uses. Also, you can deliver Cognos content using a third-party portal by configuring Portal Services.

You can configure Cognos 8 to use other resources, such as using an authentication provider and then enabling single signon for the database connection and the users.

If you use a load-balancing scheme in your environment, you can change settings to improve performance. For example, you can balance requests among dispatchers by changing their processing capacity or by setting the minimum and maximum number of processes and connections. For more information about tuning server performance, see the *Administration and Security Guide*.

If you are upgrading from ReportNet, you have several configuration options depending on if you want to continue to use your existing installation. For information about upgrade options, see "Upgrading from ReportNet, Metrics Manager, or Earlier Versions of Cognos 8" (p. 55).

Start Cognos Configuration

Use the configuration tool, Cognos Configuration, to configure Cognos 8, or to start and stop Cognos services.

Before starting Cognos Configuration, ensure that the operating environment is properly set up. For example, ensure that all variables have been set.

You should start Cognos Configuration in the last page of the installation wizard on Windows, UNIX, or Linux only if additional setup is not required. For example, if you use a database server other than Microsoft SQL for the content store, we recommend that you copy the JDBC drivers to the appropriate location before you start the configuration tool.

To start Cognos Configuration on a Windows computer,

- From the **Start** menu, click **Programs**, **Cognos 8**, **Cognos Configuration**.

To start Cognos Configuration on a UNIX or Linux computer,

- Go to the *c8_location*/bin directory and then type

  ./cogconfig.sh

Configuring Single Computer Installations

If you install all Cognos server components on one computer, some configuration tasks are required so that those components work in your Cognos environment.

Additional configuration tasks are required if the Windows modeling tools, Framework Manager, Cognos 8 Transformer, or Metric Designer, are installed on a separate computer.

If you change the value of a property, you must save the configuration and then restart the Cognos 8 service to apply the new settings to your computer.

Before you configure Cognos 8, ensure that

- all Cognos server components are installed on one computer
- a Web server is installed, configured, and running on the same computer as the Cognos 8 components
- you created the database for the content store and, if using Metric Studio, the databases for metric stores on an available computer in your network
- a Web browser is installed and configured on the same computer as Cognos 8

Use the following checklist to guide you through the required configuration tasks:

- ❑ Set the database connection properties for the content store
- ❑ Configure a mail server account
- ❑ Update file location properties, if required
- ❑ Start the Cognos 8 services
- ❑ Test the installation and configuration
- ❑ Create a metric package, if required
- ❑ Finish the configuration

After you complete these configuration tasks, you can change the default behavior of Cognos 8 (p. 193) to better suit your Cognos environment. You can also configure the Windows modeling tools, Framework Manager (p. 176), and Metric Designer (p. 188).

Set Database Connection Properties for the Content Store

For all installations not using Cognos Content Database, you must specify the database server information to ensure that Content Manager can connect to the database you use for the content store. Content Manager uses the database logon to access the content store. After you set the database connection properties, you can test the connection between Content Manager and the content store.

Ensure that you used one of the supported database servers to create the content store.

Note: Some database servers are available with advanced features. When you select an advanced database, Cognos 8 uses features of the database server to manage the connection. If you select the advanced Oracle database, for example, Cognos 8 uses enterprise-oriented Oracle features to select a listener, switch to another listener if the first listener fails, automatically reconnect to the database if the connection fails, balance connection requests among listeners, and balance connection requests among dispatchers.

Cognos 8 requires the TCP/IP protocol to access data and the content store. Ensure that the database server has the protocol set to TCP/IP.

If you are upgrading from ReportNet, configure Cognos 8 to point to the existing content store. After you save the configuration and start the Cognos 8 service, the content store is automatically upgraded and cannot be used by ReportNet. If you keep ReportNet running, you must configure Cognos 8 to point to a new content store.

Steps for Microsoft SQL Server, Oracle, DB2, and Sybase

1. On the computer where you installed Content Manager, start Cognos Configuration.
2. In the **Explorer** window, under **Data Access**, **Content Manager**, right-click **Content Store** and click **Delete**.

   This deletes the default resource. Content Manager must be configured to access only one content store.
3. Right-click **Content Manager**, and then click **New resource**, **Database**.
4. In the **Name** box, type a name for the resource.
5. In the **Type** box, select the type of database and click **OK**.

   If you are upgrading and want to use an existing content store, ensure that you select the type of database you use for the older version of ReportNet.

   If you installed more than one version of Cognos 8, you must use a different content store for each version. When a content store is used by a new version of Cognos 8, it cannot be used by an older version of ReportNet.

Tip: If you want to use Oracle Net8 keyword-value pair to manage the database connection, select **Oracle database (Advanced)**.

6. In the **Properties** window, provide values depending on your database type:
   - If you use a Microsoft SQL Server database, type the appropriate values for the **Database server with port number or instance name** and **Database name** properties.

     For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property.

     To connect to a named instance, you must specify the instance name as a JDBC URL property or a data source property. For example, you can type **localhost\instance1**. If no instance name property is specified, a connection to the default instance is created.

     Note that the properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

     jdbc:JSQLConnect://localhost\\instance1/user=sa/*more properties as required*
   - If you use a DB2 database, for the **Database name** property, type the database alias.
   - If you use an Oracle database, type the appropriate values for the **Database server and port number** and **Service name** properties.
   - If you use an advanced Oracle database, for the **Database specifier** property, type the Oracle Net8 keyword-value pair for the connection.

     Here is an example:

     (description=(address=(host=myhost)(protocol=tcp)(port=1521)(connect_data=(sid=(orcl)))))
   - If you use a Sybase database, type the appropriate values for the **Database server and port number** and **Database name** properties.
7. If you want to change the logon credentials, specify a user ID and password:
   - Click the **Value** box next to the **User ID and password** property and then click the edit button when it appears.
   - Type the appropriate values and click **OK**.
8. From the **File** menu, click **Save**.

   The logon credentials are immediately encrypted.
9. Test the connection between Content Manager and the content store.

   Tip: In the **Explorer** window, right-click the new database and click **Test**.

   Content Manager connects to the database, checks the database permissions, and creates and populates a table. The table is not deleted and is used each time that the test is repeated.

Content Manager can now create the required tables in the content store when you start the Cognos 8 service for the first time. If the connection properties are not specified correctly, you cannot connect to Cognos Connection.

If you are upgrading from ReportNet, Content Manager can now access the required tables in the content store that you used for the older version.

Specify a Mail Server Account and Notification Database

If you want to send reports by email, you must configure a mail server account. You must also specify the location of the database that is used by the notification server to store job and schedule information.

If you use a distributed installation (for example, for load balancing), you must configure all Content Manager and Application Tier Components computers to use the same database for notification.

By default, the notification server uses the same database that Content Manager uses for the content store. You can use a separate database for notification in situations where you run large volumes of batch reports and email. If so, ensure that the notification database exists and that there are no requests waiting to run. Queued requests will not be moved. All Content Manager computers must be configured to use the same notification database.

When you finish configuring a mail server account and notification database, you can test the connections to the mail server and notification database.

Tip: To be able to open reports that are sent by email, you must change the host name portion of the Gateway URI from localhost to either the IP address of the computer or the computer name. Otherwise the URL in the email will contain localhost and remote users will not be able to open the report.

If you are upgrading from ReportNet, Cognos 8 uses the mail server account and settings that were set up for ReportNet.

Steps

1. On each computer where Content Manager is installed, start Cognos Configuration.
2. In the **Explorer** window, under **Data Access**, click **Notification**.
3. In the **Properties** window, for the **SMTP mail server** property, type the host name and port of your SMTP (outgoing) mail server.
4. Click the **Value** box next to the **Account and password** property and then click the edit button when it appears.
5. Type the appropriate values in the **Value - Account and password** dialog box and then click **OK**.

   Tip: If logon credentials are not required for the SMTP server, remove the default information for the **Account and password** property. When you are prompted for confirmation to leave this property blank, click **Yes**. Ensure that the default user name has been removed. Otherwise, the default account is used and notifications will not work properly.

6. In the **Properties** window, type the appropriate value for the default sender account.

   Tip: If you use the default notification database, you do not have to perform the following two steps.

7. Identify the database that is used for notification:
   - In the Explorer window, right-click **Notification** and select **New resource, Database**.
   - Type a name for the database resource.
   - Select the type of database from the pull-down menu.
   - Click **OK**.

8. In the **Properties** window, enter the values for the notification database resource.

   For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property.

   To connect to a named instance, you must specify the instance name as a JDBC URL property or a data source property. For example, you can type **localhost\instance1**. If no instance name property is specified, a connection to the default instance is created.

   Note that the properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

   jdbc:JSQLConnect://localhost\\instance1/user=sa/*more properties as required*

9. From the **File** menu, click **Save**.

10. Test the notification and mail server connections. In the **Explorer** window right-click **Notification** and click **Test**.

    Cognos 8 tests the database connection and tests the mail server connection.

    If you have been using the content store database for notification, the schedules will be replicated in the tables of the new notification database.

Important: Ensure that the values used to identify the notification database resource are the same on all Content Manager computers. To use the default notification database, you do not have to edit the values in the **Properties** window.

Update File Location Properties

If you install Cognos 8 on Windows Vista, you must change file locations properties in Cognos Configuration so that Cognos 8 can use a single data location for all users.

Windows Vista has a security enhancement that restricts multiple users from sharing data locations. You can define environment variables and use them in Cognos Configuration when specifying file locations. This allows you to direct applicable files to an area that will be accessible by Cognos 8 users. On Windows, two environment variables are preset for users: one for all users and one for the specific user

Because the environment variables represent system root locations, we recommend that you also include the root directory name of the installation location when you specify file locations in Cognos Configuration. The default root directory for Cognos 8 is c8.

Steps

1. Start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, click **Deployment files location**.
4. Replace the relative path element, "..", with the appropriate environment variable and root directory, using the following suggested environment variables:
   - For a single file location per user, %LOCALAPPDATA%
   - For a single file location for all users on the computer, %PUBLIC%

   For example,

   To set a single file location per user, specify the path %LOCALAPPDATA%/c8/deployment.
5. Repeat step 4 for the following properties:
   - Under **Environment**,

     - **Data files location**

     - **Map files location**

     - **Temporary files location**
   - Under **Environment**, **Logging**, **File**,

     - **Log file location**
   - Under **Cryptography**,

     - **Common symmetric key store location**
   - Under **Cryptography**, **Cognos**,

     - **Certificate location**

     - **Signing key store location**

     - **Encryption key store location**
6. From the **File** menu, click **Save**.

The environment variables are resolved when the file locations are accessed during system activities.

Start the Cognos 8 Services

To register the Cognos 8 service so that users can access it through Cognos Connection, you must start the services. Before you start the services, test the configuration by using the test feature in Cognos Configuration.

Before you can use Framework Manager, Cognos 8 Transformer, or Metric Designer, you must start the Cognos 8 service. On Windows, the Cognos 8 service is configured to start automatically by default. On UNIX and Linux, to start the Cognos 8 process automatically, you must configure the process as a daemon. For more information, see your operating system documentation.

You must install and configure both the server components of Cognos 8 and Framework Manager before you can use Cognos 8 for reporting.

Note: Cognos 8 cannot access any reporting data unless the data is first packaged in and published from Framework Manager.

Steps

1. Start Cognos Configuration.
2. Ensure that you save your configuration, otherwise you cannot start the Cognos 8 service.

   If you are upgrading, a message appears indicating that configuration files were detected and upgraded to the new version.
3. From the **Actions** menu, click **Test**.

   Cognos Configuration checks the CSK availability, tests the namespace configuration, and tests the connections to the content store and logging database.

   If you are using the notification database and the mail server, they are tested as well.

   Tip: If **Test** is not available for selection, in the **Explorer** window, click **Local Configuration**.
4. If the test fails, reconfigure the affected properties and then test again.

   You can test individual services by right-clicking the service in the **Explorer** panel and selecting **Test**.

   Do not start the service until all tests pass.
5. From the **Actions** menu, click **Start**.

   It may take a few minutes for the Cognos 8 service to start.

   This action starts all installed services that are not running. If you want to start a particular service, select the service node in the **Explorer** window and then click **Start** from the **Actions** menu.

Test the Installation and Configuration

You can test your configuration settings by running the test feature as you configure Cognos 8. After you have completed the configuration and started the services, you can test the installation by opening Cognos Connection. If you installed Framework Manager or Metric Designer, you can test it by starting the application and creating a project.

If you installed Metric Studio and you have created a package, you have already tested your installation and configuration. You can create a metric package only if Metric Studio is installed and configured properly.

Steps

1. Open a Web browser.
2. Test the availability of the dispatcher by typing

   http://*host_name:port*/p2pd/servlet

   If the response includes the string State: Running, the dispatcher is available.
3. Open Cognos Connection by typing one the following, where cognos8 is the virtual directory you created when you configured the Web server.
   - For the CGI gateway:

     http://*host_name:port*/cognos8
   - For an ISAPI gateway:

     http://*host_name:port*/cognos8/isapi
   - For Apache Connector on Windows:

     http://*host_name:port*/cognos8/cgi-bin/mod_cognos.dll
   - For Apache Connector on Solaris or AIX:

     http://*host_name:port*/cognos8/cgi-bin/mod_cognos.so
   - For Apache Connector on HP-UX PA-RISC:

     http://*host_name:port*/cognos8/cgi-bin/mod_cognos.sl
   - For Apache Connector on HP-UX IA or Linux:

     http://*host_name:port*/cognos8/cgi-bin/mod2_cognos.so
   - For a gateway servlet:

     http://*host_name:port/context_root*/servlet/ Gateway

   It may take a few minutes for the Web page to open. If you see the **Welcome** page of Cognos Connection, your installation is working.

Step for Framework Manager

- To start Framework Manager, from the **Start** menu, click **Programs**, **Cognos 8**, **Framework Manager**.

  You may be prompted to upgrade if the model schema version is older than the currently supported version.

If you see the **Welcome** page of Framework Manager, your installation is working.

Step for Cognos 8 Transformer

- To start Cognos 8 Transformer, from the **Start** menu, click **Programs**, **Cognos 8**,**Transformer**.

  To start Cognos 8 Transformer manually, double-click the following file in the *c8_location*\bin directory:

  - For Windows, cogtr.exe
  - For UNIX or Linux, cogtr.sh

  If you see the **Transformer** window, your installation is working.

Step for Metric Designer

- To start Metric Designer, from the **Start** menu, click **Programs**, **Cognos 8**, **Metric Designer**.

  If you see the **Welcome** page of Metric Designer, your installation is working.

Create a Metric Package

Before users can use Metric Studio, you must create at least one metric package using the New Metric Package wizard. A metric package is a Cognos Connection representation of a Metric Studio application. A metric package contains connection information, reports, and metric management tasks for that application. The metric package content is stored in a metric store.

You open the New Metric Package wizard from the toolbar in Cognos Connection. Use the wizard to define the metric package name and the data source connection to the metric store. For a new metric store, you also provide the information necessary to initialize the database, including the start and end dates of the fiscal year. If the database was used with an earlier version of Metric Studio 8.1 or later, you can use the wizard to upgrade the metric store.

Before you can use the New Metric Package wizard, you must have access to a metric store used with Metrics Manager version 2.0 or later or you must create a database for a new metric store (p. 124).

Steps

1. Start Cognos Connection.
2. Click the **New metric package** button .
3. Type a name and description for the Metric Studio application to represent this metric package, and click **Next**.
4. Click **New data source**.
5. Type a name and description for the data source connection for the metric store that contains the content for this metric package, and click **Next**.
6. In the **Type** box, click the database type.

7. Select the isolation level, and click **Next**.
8. Specify the information required for your database type:
   - For a Microsoft SQL Server database, type the name of the database server and the database. Under **Signons**, select the **Password** and **Create a signon that the Everyone strategy can use** check boxes, and type the user ID and password of the user account with access to the database.
   - For an Oracle database, type the connection string. Select **User ID**, select the **Password** and **Create a signon that the Everyone strategy can use** check boxes, and type the user ID and password of the user account with access to the database.
   - For a DB2 database, type the name of the database, the connection string, and the collation sequence. Select **User ID**, select the **Password** and **Create a signon that the Everyone strategy can use** check boxes, and type the user ID and password of the user account with access to the database.

   Tip: To test whether the parameters are correct, click **Test**.
9. Click **Next** and then click **Finish**.
10. Click the new data source and click **Next**.
11. Click **Next** and follow the prompts to provide the information necessary to initialize the database. When you see the page that summarizes the data source details and the metric store settings, click **Initialize**.
12. Select **Open this package with Metric Studio after closing the wizard** and then click **Finish**.

Metric Studio opens and the new metric package is displayed in Cognos Connection. For information about managing the metric store, including how to load data, see the Cognos 8 *Administration and Security Guide*.

Steps Using an Existing Metric Store

1. Start Cognos Connection.
2. Click the **New metric package** button .
3. Type the name and description for the Metric Studio application to represent this metric package and click **Next**.
4. Click **New data source**.
5. Type the name and description for the data source connection for the metric store that contains the content for this metric package, and click **Next**.
6. In the **Type** box, click the database type and click **Next**.
7. Specify the information required for your database type:
   - For a Microsoft SQL Server database, type the name of the database server and the database. Under **Signons**, select the **Password** and **Create a signon that the Everyone group can use**

check boxes, and type the user ID and password of the user account with access to the database.

- For an Oracle database, type the connection string. Under **User ID**, select the **Password** and **Create a signon that the Everyone group can use** check boxes, and type the user ID and password of the user account with access to the database.
- For a DB2 database, type the name of the database and the connection string. Select **User ID**, select the **Password** and **Create a signon that the Everyone group can use** check boxes, and type the user ID and password of the user account with access to the database.

Tip: To test whether the parameters are correct, click **Test**.

8. Click **Next**.
9. Select **Open this package with Metric Studio after closing the wizard** and then click **Finish**.

   Metric Studio opens and the new metric package is displayed in Cognos Connection.
10. Click the new data source and click **Next**.
11. Click **Upgrade**.

    The wizard updates the database schemas and other information.

For information about managing the metric store, see the *Administration and Security Guide*.

Finishing the Configuration

After you complete the required configuration tasks, you can perform some additional configuration tasks to customize the behavior of Cognos 8 components to better suit your Cognos environment (p. 193). You can also add resources, such as configuring Cognos 8 components to use an authentication provider (p. 255).

We recommend that you specify the amount of resources the Cognos 8 service uses to ensure that performance is optimized.

Configuring Distributed Installations

To improve performance or to enhance security, you can install any one of the following components on a separate computer:

- gateway
- Application Tier Components
- Content Manager
- Cognos Content Database

For information about planning a distributed installation, see the *Architecture and Deployment Guide*.

You can install the Application Tier Components, gateway, and Content Manager on multiple computers.

If you are upgrading from ReportNet, all the distributed components must be the same version of Cognos 8. If you install Cognos 8 in new locations, you must update the locations using Cognos Configuration.

If you install Cognos 8 components on more than one computer, you must configure environment properties so that the distributed components can communicate with each other:

- The Content Manager computers must know the location of the content store, the other Content Manager computers, and the database that is used for notification.
- The gateway computer must know the location of at least one dispatcher.

  The dispatcher should be located on a report server computer.
- The Application Tier Components computer must know the location of the Content Manager computers and the database to use for job and schedule information.

You must also configure cryptographic properties to ensure that each computer uses the same settings.

In a distributed environment, the sequence in which you configure computers is important. You must configure and then start the services on at least one computer where you installed Content Manager before you configure other computers in your Cognos environment. You must configure the gateway computer last so that cryptographic keys are shared and secure communication can take place among the three components. The server specified for the External Dispatcher URI property on the gateway computer must be the last server that you start.

Use the following checklist to guide you through the required configuration tasks:

- ❑ Configure the Content Manager computers.
- ❑ Configure the Application Tier Components computers.
- ❑ Configure the gateway computers.
- ❑ Configure the Framework Manager computers, if required.
- ❑ Configure the Cognos 8 Transformer computers, if required.
- ❑ Configure the Metric Designer computers, if required.
- ❑ Create a metric package, if required.
- ❑ Start the Cognos 8 services.
- ❑ Test the installation and configuration.
- ❑ Finish the configuration.

After you complete these configuration tasks, you can configure Cognos 8 to use an authentication provider (p. 255) or change the default behavior of Cognos 8 components (p. 193) to better suit your Cognos environment.

We recommend that you specify the amount of resources the Cognos 8 service uses to ensure that performance is optimized.

Configuring Content Manager Computers

In a distributed installation, at least one of the computers where you installed Content Manager must be configured, running and accessible before you configure other computers in your Cognos environment. This ensures that the certificate authority service, which is installed with Content Manager, is available to issue certificates to other Cognos computers.

Your installation may include more than one Content Manager, each on a different computer. One Content Manager computer is active and one or more Content Manager computers are on standby. The standby Content Manager computers are for failover protection. If the active Content Manager computer is not available because of a software or hardware failure, a standby Content Manager computer becomes active and requests are directed to it.

When the active Content Manager fails, unsaved session data is lost. When another Content Manager becomes active, users may be prompted to log on.

The first Content Manager computer to be started becomes the default active Content Manager. You can designate another Content Manager computer as default active, using the Administration tool. For more information about activating a Content Manager service, see the *Administration and Security Guide*.

To support failover protection, you must synchronize the system clocks on the Content Manager computers. If you use the default CGI gateway, you must also configure Cognos 8 to use an ISAPI gateway instead.

Before you configure Content Manager, ensure that you created the database for the content store on an available computer in your network.

If you install Cognos Content Database on the same computer as you install Content Manager, Content Manager will be configured to use Cognos Content Database by default. If you install Cognos Content Database on another computer, you must set the database connection properties for Content Manager to connect to the computer where you installed Cognos Content Database. If you do not install Cognos Content Database, the default connection settings are for a Microsoft SQL Server database.

If you install Cognos Content Database on the same computer as Content Manager, and you later decide to use another database for your content store, you must uninstall Cognos Content Database.

If you are upgrading from ReportNet, you can use the existing configuration data. However, some features in Cognos 8 are new. We recommend that you configure the new features.

Use the following checklist to guide you through the required configuration tasks for the Content Manager computers:

- ❑ Set the database connection properties for the content store.
- ❑ Specify a mail server account and notification database.
- ❑ Configure the environment properties.
- ❑ Update file location properties, if required.

- ❑ Start the Cognos 8 services.

Set Database Connection Properties for the Content Store

You must specify the database server information to ensure that Content Manager can connect to the database you use for the content store. Content Manager uses the database logon to access the content store. After you set the database connection properties, you can test the connection between Content Manager and the content store.

If you installed Cognos Content Database on a different computer from where you installed Content Manager, you must set the database connection properties for Cognos Content Database. If you installed Cognos Content Database on the same computer as Content Manager, Content Manager is configured to use Cognos Content Database using the default values. If you install Cognos Content Database on the same computer as Content Manager, and you later decide to use another database for your content store, you must uninstall Cognos Content Database.

Ensure that you used one of the supported database servers to create the content store.

Note: Some database servers are available with advanced features. When you select an advanced database, Cognos 8 components use features of the database server to manage the connection. If you select the advanced Oracle database, for example, Cognos 8 components use enterprise-oriented Oracle features to select a listener, switch to another listener if the first listener fails, automatically reconnect to the database if the connection fails, balance connection requests among listeners, and balance connection requests among dispatchers.

Cognos 8 components require the TCP/IP protocol to access data and the content store. Ensure that the database server has the protocol set to TCP/IP.

If you are using Oracle, you do not have to install an Oracle client on the same computer as Content Manager. Content Manager, however, does require an Oracle JDBC driver called ojdbc14.jar. The driver is available from an Oracle client or server install, and it can also be downloaded from the Oracle technology Web site (http://www.oracle.com/technology). The ojdbc14.jar driver file must be copied to the *c8_location*\p2pd\WEB-INF\lib directory where you installed the Content Manager. If the directory contains the classes12.jar file, you must delete it before installing the ojdbc14.jar file.

If you are upgrading from ReportNet, configure Cognos 8 to point to the existing content store. After you save the configuration and start the Cognos 8 service, the content store is automatically upgraded and cannot be used by ReportNet. If you keep ReportNet, you must configure Cognos 8 to point to a new content store.

Steps for Cognos Content Database

1. On the computer where you installed Content Manager, start Cognos Configuration.
2. In the **Explorer** window, under **Data Access**, **Content Manager**, right-click **Content Store**, and then click **Delete**. Click **Yes** to confirm the deletion.

   This action deletes the default database.
3. Right-click **Content Manager**, and then click **New resource, Database**.

4. In the **Properties** window, configure Cognos 8 to use Cognos Content Database as the content store:
   - For **Name**, type **cm**.
   - For **Database server and port number**, type the name of the computer where you installed Cognos Content Database.
   - For **User ID and password**, click the edit button and specify cognos for both the userid and password to access Cognos Content Database.

   We recommend that you change the default user ID and password after configuring the new resource. For information about changing default values, see "Change Default User and Password for Cognos Content Database" (p. 194).
5. From the **File** menu, click **Save**.

   The logon credentials are immediately encrypted.
6. In the **Explorer** window, right-click **Content Store** and click **Test** to test the connection between Content Manager and the content store.

   You must start the Cognos Content Database service on the computer where it is installed before the test will succeed.

   Content Manager connects to the database, checks the database permissions, and creates and populates a table. The table is not deleted and is used each time that the test is repeated.

Steps for Microsoft SQL Server, Oracle, DB2, and Sybase

1. On the computer where you installed Content Manager, start Cognos Configuration.
2. In the **Explorer** window, under **Data Access**, **Content Manager**, right-click **Content Store** and click **Delete**.

   This deletes the default resource. Content Manager must be configured to access only one content store.
3. Right-click **Content Manager**, and then click **New resource**, **Database**.
4. In the **Name** box, type a name for the resource.
5. In the **Type** box, select the type of database and click **OK**.

   If you are upgrading and want to use an existing content store, ensure that you select the type of database you use for the older version of ReportNet.

   If you installed more than one version of Cognos 8, you must use a different content store for each version. When a content store is used by a new version of Cognos 8, it cannot be used by an older version of ReportNet.

   Tip: If you want to use Oracle Net8 keyword-value pair to manage the database connection, select **Oracle database (Advanced)**.
6. In the **Properties** window, provide values depending on your database type:

- If you use a Microsoft SQL Server database, type the appropriate values for the **Database server with port number or instance name** and **Database name** properties.

  For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property.

  To connect to a named instance, you must specify the instance name as a JDBC URL property or a data source property. For example, you can type **localhost\instance1**. If no instance name property is specified, a connection to the default instance is created.

  Note that the properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

  jdbc:JSQLConnect://localhost\\instance1/user=sa/*more properties as required*

- If you use a DB2 database, for the **Database name** property, type the database alias.
- If you use an Oracle database, type the appropriate values for the **Database server and port number** and **Service name** properties.
- If you use an advanced Oracle database, for the **Database specifier** property, type the Oracle Net8 keyword-value pair for the connection.

  Here is an example:

  (description=(address=(host=myhost)(protocol=tcp)(port=1521)(connect_data=(sid=(orcl)))))
- If you use a Sybase database, type the appropriate values for the **Database server and port number** and **Database name** properties.

7. If you want to change the logon credentials, specify a user ID and password:
   - Click the **Value** box next to the **User ID and password** property and then click the edit button when it appears.
   - Type the appropriate values and click **OK**.
8. From the **File** menu, click **Save**.

   The logon credentials are immediately encrypted.
9. Test the connection between Content Manager and the content store.

   Tip: In the **Explorer** window, right-click the new database and click **Test**.

   Content Manager connects to the database, checks the database permissions, and creates and populates a table. The table is not deleted and is used each time that the test is repeated.

Content Manager can now create the required tables in the content store when you start the Cognos 8 service for the first time. If the connection properties are not specified correctly, the tables are not created and you cannot connect to Cognos Connection.

If you are upgrading from ReportNet, Content Manager can now access the required tables in the content store that you used for ReportNet.

Specify a Mail Server Account and Notification Database

If you want to send reports by email, you must configure a mail server account. You must also specify the location of the database that is used by the notification server to store job and schedule information.

If you use a distributed installation (for example, for load balancing), you must configure all Content Manager and Application Tier Components computers to use the same database for notification.

By default, the notification server uses the same database that Content Manager uses for the content store. You can use a separate database for notification in situations where you run large volumes of batch reports and email. If so, ensure that the notification database exists and that there are no requests waiting to run. Queued requests will not be moved. All Content Manager computers must be configured to use the same notification database.

When you finish configuring a mail server account and notification database, you can test the connections to the mail server and notification database.

Tip: To be able to open reports that are sent by email, you must change the host name portion of the Gateway URI from localhost to either the IP address of the computer or the computer name. Otherwise the URL in the email will contain localhost and remote users will not be able to open the report.

If you are upgrading from ReportNet, Cognos 8 uses the mail server account and settings that were set up for the older version.

Steps

1. On each computer where Content Manager is installed, start Cognos Configuration.
2. In the **Explorer** window, under **Data Access**, click **Notification**.
3. In the **Properties** window, for the **SMTP mail server** property, type the host name and port of your SMTP (outgoing) mail server.
4. Click the **Value** box next to the **Account and password** property and then click the edit button when it appears.
5. Type the appropriate values in the **Value - Account and password** dialog box and then click **OK**.

   Tip: If logon credentials are not required for the SMTP server, remove the default information for the **Account and password** property. When you are prompted for confirmation to leave this property blank, click **Yes**. Ensure that the default user name has been removed. Otherwise, the default account is used and notifications will not work properly.
6. In the **Properties** window, type the appropriate value for the default sender account.

   Tip: If you use the default notification database, you do not have to perform the following two steps.
7. Identify the database that is used for notification:
   - In the Explorer window, right-click **Notification** and select **New resource**, **Database**.

- Type a name for the database resource.
- Select the type of database from the pull-down menu.
- Click **OK**.

8. In the **Properties** window, enter the values for the notification database resource.

   For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property.

   To connect to a named instance, you must specify the instance name as a JDBC URL property or a data source property. For example, you can type **localhost\instance1**. If no instance name property is specified, a connection to the default instance is created.

   Note that the properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

   jdbc:JSQLConnect://localhost\\instance1/user=sa/*more properties as required*

9. From the **File** menu, click **Save**.

10. Test the notification and mail server connections. In the **Explorer** window right-click **Notification** and click **Test**.

    Cognos 8 tests the database connection and tests the mail server connection.

    If you have been using the content store database for notification, the schedules will be replicated in the tables of the new notification database.

Important: Ensure that the values used to identify the notification database resource are the same on all Content Manager computers. To use the default notification database, you do not have to edit the values in the **Properties** window.

Configure Environment Properties for Content Manager Computers

After installing Content Manager on the computers you are using for failover protection, you must configure Content Manager on those computers. If you installed more than one Content Manager, you must list all Content Manager URIs on each Content Manager computer. If you are upgrading, you must also add the standby Content Manager URIs to the original Content Manager computer.

After you complete the required configuration tasks, the certificate authority service is available to issue certificates to other Cognos computers. You can then perform the required configuration tasks on other computers, such as the Application Tier Components computer and gateway computers. Otherwise you can continue to configure the Content Manager computers by changing the default property settings (p. 193) so that they better suit your environment. For example, you can configure Cognos 8 components to use an authentication provider (p. 255), enable and disable services (p. 203) on the Content Manager computers, or change global settings (p. 221).

Important: If you change global settings on one Content Manager computer, you must make the same changes on the other Content Manager computers.

Steps for the First Content Manager Computer

1. On the Content Manager computer that you want to designate as the default active Content Manager, start Cognos Configuration.

   Tip: We recommend that you use the computer with the highest processor speed for the default active Content Manager.

2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, click the value for **Content Manager URIs** and then click the edit button.
4. Specify the URIs for the other Content Manager computers:
   - In the **Value - Content Manager URIs** dialog box, click **Add**.
   - In the blank row of the table, click and then type the full URI of the Content Manager computer.

     Do not delete the first value in the table. This value identifies the local Content Manager computer and is required.
   - Repeat the previous two bulleted steps for each URI to be added.

     Important: You must include all Content Manager URIs in the list.
   - Click **OK**.
5. In the **Explorer** window, under **Security**, click **Cryptography**.
6. In the **Properties** window, under **CSK settings**, set **Store symmetric key locally** to **True**.
7. From the **File** menu, click **Save**.

Steps for Standby Content Manager Computers

1. Ensure that you already configured the Environment properties on at least one Content Manager computer and that Cognos 8 components are running on that computer.
2. On the standby Content Manager computer, start Cognos Configuration.
3. In the **Explorer** window, click **Environment**.
4. In the **Properties** window, click the value for **Content Manager URIs** and then click the edit button.
5. Specify the URIs for the other Content Manager computers:
   - In the **Value - Content Manager URIs** dialog box, click **Add**.
   - In the blank row of the table, click and then type the full URI of the Content Manager computer.

Do not delete the first value in the table. This value identifies the local Content Manager computer and is required.

- Repeat the previous two bulleted steps for each URI to be added.

  Important: You must include all Content Manager URIs in the list.

- Click **OK**.

6. In the **Explorer** window, under **Security**, click **Cryptography**.
7. In the **Explorer** window, under **Security**, **Cryptography**, click **Cognos**, the default cryptographic provider.
8. Under the **Certificate Authority settings** property group, set the **Password** property to match what you configured on the default active Content Manager computer.
9. Ensure that all other cryptographic settings match what you configured on the default active Content Manager computer.
10. In the **Explorer** window, under **Data Access**, **Content Manager**, click **Content Store**.
11. Ensure that the values for all of the properties match what you configured on the default active Content Manager computer.
12. From the **File** menu, click **Save**.

Update File Location Properties

If you install Cognos 8 in an environment that includes Windows Vista, you must change file locations properties in Cognos Configuration so that Cognos 8 can use a single data location for all users. The changes must be made on all computers where Cognos 8 components are installed.

Windows Vista has a security enhancement that restricts multiple users from sharing data locations. You can define environment variables and use them in Cognos Configuration when specifying file locations. This allows you to direct applicable files to an area that will be accessible by Cognos 8 users.

Because the environment variables represent system root locations, we recommend that you also include the root directory name of the installation location when you specify file locations in Cognos Configuration. The default root directory for Cognos 8 is c8.

Environment variables must be set prior to starting Cognos 8. On UNIX and Linux, they can be set in the administrator login scripts. On Windows, two environment variables are preset for users: one for all users and one for the specific user.

Steps

1. Start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, click **Deployment files location**.

4. Replace the relative path element, "..", with the appropriate environment variable and root directory:
   - On Windows, use the preset environment variables as shown in the table.

Operating system	Per user	All users
Windows XP	%APPDATA%	%ALLUSERSPROFILE%
Windows Vista	%LOCALAPPDATA%	%PUBLIC%

   - On UNIX, use the environment variables that you set in advance.

   For example,

   On Windows XP, to set a single file location for all users, specify %ALLUSERSPROFILE%/c8/deployment.

   On UNIX, if you set an environment variable such as MYHOME for single users, specify $MYHOME/c8/deployment.

5. Repeat step 4 for the following properties:
   - Under **Environment**,

     - **Data files location**

     - **Map files location**

     - **Temporary files location**

   - Under **Environment**, **Logging**, **File**,

     - **Log file location**

   - Under **Cryptography**,

     - **Common symmetric key store location**

   - Under **Cryptography**, **Cognos**,

     - **Certificate location**

     - **Signing key store location**

     - **Encryption key store location**

6. From the **File** menu, click **Save**.

The environment variables are resolved when the file locations are accessed during system activities.

You are now ready to start the Cognos 8 services on the Content Manager computer or computers. As soon as the services start on the first Content Manager computer, the computer becomes the default active Content Manager. If you configured Cognos 8 with standby Content Manager computers and you use the default CGI gateway, you must configure Cognos 8 to use an ISAPI gateway. For more information, see "Changing the Gateway" (p. 231).

Configuring Application Tier Components Computers

You can install the Application Tier Components component on one or more computers, depending on your environment.

If you installed more than one Content Manager, you must list all Content Manager URIs on each report server computer.

If you are upgrading from ReportNet, Cognos 8 uses the existing configuration data for the Application Tier Components computers. However, if you installed the Application Tier Components in a new location, you must configure the environment properties.

Ensure that the computer where you installed the active Content Manager is configured and available before you configure Application Tier Components computers.

If Content Manager and the Application Tier Components are installed on separate computers, on the Application Tier Components computer, you must do the following:

- Specify a mail server account and notification database.
- Configure Environment properties.
- Update file location properties, if required.
- Start the Cognos 8 services.

Other configuration tasks are optional and may be performed later.

Specify a Mail Server Account and Notification Database

If you want to send reports by email, you must configure a mail server account. You must also specify the location of the database that is used by the notification server to store job and schedule information.

When you finish configuring a mail server account and notification database, you can test the connections to the mail server and notification database.

If you are upgrading from ReportNet, Cognos 8 uses the mail server account and settings that were set up for the older version.

You must configure all report server computers to use the same database for notification. You must use the same database that is used for notification on Content Manager computers.

Tip: To be able to open reports that are sent by email, you must change the host name portion of the Gateway URI from localhost to either the IP address of the computer or the computer name. Otherwise the URL in the email will contain localhost and remote users will not be able to open the report.

Steps

1. On each computer where Content Manager is installed, start Cognos Configuration.
2. In the **Explorer** window, under **Data Access**, click **Notification**.
3. In the **Properties** window, for the **SMTP mail server** property, type the host name and port of your SMTP (outgoing) mail server.

4. Click the **Value** box next to the **Account and password** property and then click the edit button when it appears.
5. Type the appropriate values in the **Value - Account and password** dialog box and then click **OK**.

   Tip: If logon credentials are not required for the SMTP server, remove the default information for the **Account and password** property. When you are prompted for confirmation to leave this property blank, click **Yes**. Ensure that the default user name has been removed. Otherwise, the default account is used and notifications will not work properly.
6. In the **Properties** window, type the appropriate value for the default sender account.

   Tip: If you use the default notification database, you do not have to perform the following two steps.
7. Identify the database that is used for notification:
   - In the Explorer window, right-click **Notification** and select **New resource**, **Database**.
   - Type a name for the database resource.
   - Select the type of database from the pull-down menu.
   - Click **OK**.
8. In the **Properties** window, enter the values for the notification database resource.

   For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property.

   To connect to a named instance, you must specify the instance name as a JDBC URL property or a data source property. For example, you can type **localhost\instance1**. If no instance name property is specified, a connection to the default instance is created.

   Note that the properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

   jdbc:JSQLConnect://localhost\\instance1/user=sa/*more properties as required*
9. From the **File** menu, click **Save**.
10. Test the notification and mail server connections. In the **Explorer** window right-click **Notification** and click **Test**.

    Cognos 8 tests the database connection and tests the mail server connection.

    If you have been using the content store database for notification, the schedules will be replicated in the tables of the new notification database.

Configure Environment Properties for Application Tier Components Computers

If you install the Application Tier Components component on a different computer than Content Manager, you must configure the Application Tier Components computer so that it knows the location of Content Manager. The distributed components can then communicate with each other.

Steps

1. Start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, specify the appropriate value for the **Gateway URI**, by changing the **localhost** portion to the name of the gateway computer.
4. In the **Properties** window, click the value for **Content Manager URIs** and then click the edit button.
5. Change the localhost portion of the existing URI to the name of any Content Manager computer.
6. Specify the URIs for the remaining Content Manager computers:
   - In the **Value - Content Manager URIs** dialog box, click **Add**.
   - In the blank row of the table, click and then type the full URI of the Content Manager computer.
   - Repeat the previous two bulleted steps for each URI to be added.

     Important: You must include all Content Manager URIs in the list.
   - Click **OK**.
7. In the **Explorer** window, under **Security**, **Cryptography**, click **Cognos**, the default cryptographic provider.
8. Under the **Certificate Authority settings** property group, set the **Password** property to match what you configured on the default active Content Manager computer.
9. Ensure that all other cryptographic settings match what you set on the default active Content Manager computer.
10. From the **File** menu, click **Save**.

Update File Location Properties

If you install Cognos 8 in an environment that includes Windows Vista, you must change file locations properties in Cognos Configuration so that Cognos 8 can use a single data location for all users. The changes must be made on all computers where Cognos 8 components are installed.

Windows Vista has a security enhancement that restricts multiple users from sharing data locations. You can define environment variables and use them in Cognos Configuration when specifying file locations. This allows you to direct applicable files to an area that will be accessible by Cognos 8 users.

Because the environment variables represent system root locations, we recommend that you also include the root directory name of the installation location when you specify file locations in Cognos Configuration. The default root directory for Cognos 8 is c8.

The environment variable must match the one that is used for file locations on the Content Manager computers.

Steps

1. Start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, click **Deployment files location**.
4. Replace the relative path element, "..", with the appropriate environment variable and root directory:
   - On Windows, use the preset environment variables as shown in the table.

Operating system	Per user	All users
Windows XP	%APPDATA%	%ALLUSERSPROFILE%
Windows Vista	%LOCALAPPDATA%	%PUBLIC%

   - On UNIX, use the environment variables that you set in advance.

   For example,

   On Windows XP, to set a single file location for all users, specify %ALLUSERSPROFILE%/c8/deployment.

   On UNIX, if you set an environment variable such as MYHOME for single users, specify $MYHOME/c8/deployment.
5. Repeat step 4 for the following properties:
   - Under **Environment**,

     - **Data files location**

     - **Map files location**

     - **Temporary files location**
   - Under **Environment**, **Logging**, **File**,

     - **Log file location**
   - Under **Cryptography**,

     - **Common symmetric key store location**
   - Under **Cryptography**, **Cognos**,

- **Certificate location**
- **Signing key store location**
- **Encryption key store location**

6. From the **File** menu, click **Save**.

The environment variables are resolved when the file locations are accessed during system activities.

You are now ready to start the Cognos 8 services on the Application Tier Components computer. After you complete the required configuration tasks for each Application Tier Components computer in your environment, you can perform the required configuration tasks on other computers, such as the gateway computers. Otherwise you can continue to configure the Application Tier Components computers by changing the default property settings so that they better suit your environment. For example, you can enable and disable services (p. 203), configure where to send log messages (p. 215) or configure the amount of resources the Cognos 8 service uses (p. 204).

Configure Gateway Computers

You can install the gateway on one or more computers, depending on your environment.

If you are upgrading from ReportNet, Cognos 8 uses the existing configuration data for the gateway computers. However, if you installed the gateway in a new location, you must configure the gateway.

Ensure that the computer where you installed the active Content Manager is configured and available before you configure gateway computers.

If Content Manager and the gateway are installed on separate computers, on the gateway computer, you must do the following:

- Configure environment properties.
- Update file locations, if required.
- Start the Cognos 8 services.

Configure Environment Properties for Gateway Computers

You can install the gateway on one or more Web server computers.

If you install the gateway component on a different computer than Content Manager or Application Tier Components, you must configure the gateway computer so that it knows the location of a dispatcher. A dispatcher is installed on every Content Manager and Application Tier Components computer. We recommend that the gateway use the dispatcher on a Application Tier Components computer.

For failover protection, you can configure more than one dispatcher for a gateway computer. When multiple dispatchers are configured, requests are normally routed to the first dispatcher in the list. If this dispatcher becomes unavailable, the gateway determines the next functioning dispatcher on the list and routes requests there. The primary dispatcher status is monitored by the gateway, and requests are routed back to this component when it returns to service.

After you do the required configuration tasks, the gateway computer can work in your environment.

Ensure that the computers where you installed Content Manager are configured and the default active Content Manager computer is available before you configure gateway computers.

Steps

1. Start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, under **Gateway Settings**, specify the values for **Dispatcher URIs for the gateway**:
   - Click in the value column.
   - Click the edit button.
   - Change the localhost portion of the URI to the name or IP address of an Application Tier Components computer.

     Tip: If you want to send requests to the dispatcher from an SDK application or a Cognos 8 modeling tool that is outside of a network firewall, we recommend that you connect to a dedicated gateway that is configured to connect to the dispatcher using the Internal dispatcher URI for your environment (for example, http://localhost:9300/p2pd/servlet/dispatch). For security reasons, the default setting for the Dispatcher URI for gateway property prevents the dispatcher from accepting requests for an SDK application or modeling tool that is outside the firewall. Ensure that you configure appropriate security for this dedicated gateway. Do not change your main gateway to use the Internal dispatcher URI. Doing so will reduce the security of the Cognos 8 portal and studios. For more information about the modeling tool and network firewalls, see "Firewall Considerations" (p. 32).
   - If you want to add another URI, click **Add** and change the localhost portion of the new URI to the name or IP address of another Application Tier Components computer.

     Tip: If you want to use the dispatcher on a standby Content Manager computer, ensure that you add it after you add the Application Tier Components computers. If you add the dispatcher from the active Content Manager computer, ensure that it is last in the list.
   - After you specify all the URIs, click **OK**.
4. In the **Explorer** window, under **Security**, **Cryptography**, click **Cognos**, the default cryptographic provider.
5. Under the **Certificate Authority settings** property group, set the **Password** property to match what you configured on the default active Content Manager computer.
6. Ensure that all other cryptographic settings match what you set on the default active Content Manager computer.
7. Test that the symmetric key can be retrieved. In the **Explorer** window, right-click **Cryptography** and click **Test**.

   Cognos 8 components check the CSK availability.
8. From the **File** menu, click **Save**.

Update File Location Properties

If you install Cognos 8 in an environment that includes Windows Vista, you must change file locations properties in Cognos Configuration so that Cognos 8 can use a single data location for all users. The changes must be made on all computers where Cognos 8 components are installed.

Windows Vista has a security enhancement that restricts multiple users from sharing data locations. You can define environment variables and use them in Cognos Configuration when specifying file locations. This allows you to direct applicable files to an area that will be accessible by Cognos 8 users.

Because the environment variables represent system root locations, we recommend that you also include the root directory name of the installation location when you specify file locations in Cognos Configuration. The default root directory for Cognos 8 is c8.

The environment variable must match the one that is used for file locations on the Content Manager computers.

Steps

1. Start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, click **Deployment files location**.
4. Replace the relative path element, "..", with the appropriate environment variable and root directory:
   - On Windows, use the preset environment variables as shown in the table.

Operating system	Per user	All users
Windows XP	%APPDATA%	%ALLUSERSPROFILE%
Windows Vista	%LOCALAPPDATA%	%PUBLIC%

   - On UNIX, use the environment variables that you set in advance.

   For example,

   On Windows XP, to set a single file location for all users, specify %ALLUSERSPROFILE%/c8/deployment.

   On UNIX, if you set an environment variable such as MYHOME for single users, specify $MYHOME/c8/deployment.
5. Repeat step 4 for the following properties:
   - Under **Environment**,

     - **Data files location**

     - **Map files location**

- **Temporary files location**

- Under **Environment, Logging, File,**

  - **Log file location**

- Under **Cryptography,**

  - **Common symmetric key store location**

- Under **Cryptography, Cognos,**

  - **Certificate location**

  - **Signing key store location**

  - **Encryption key store location**

6. From the **File** menu, click **Save**.

The environment variables are resolved when the file locations are accessed during system activities.

You are now ready to start the Cognos 8 services on the Gateway computer. After you complete the required configuration tasks for each gateway computer in your environment, you can continue to configure the gateway computers by changing the default property settings so that they better suit your environment. For example, you can configure a gateway to use a namespace.

Create a Metric Package

Before users can use Metric Studio, you must create at least one metric package using the New Metric Package wizard. A metric package is a Cognos Connection representation of a Metric Studio application. A metric package contains connection information, reports, and metric management tasks for that application. The metric package content is stored in a metric store.

You open the New Metric Package wizard from the toolbar in Cognos Connection. Use the wizard to define the metric package name and the data source connection to the metric store. For a new metric store, you also provide the information necessary to initialize the database, including the start and end dates of the fiscal year. If the database was used with an earlier version of Metric Studio 8.1 or later, you can use the wizard to upgrade the metric store.

Before you can use the New Metric Package wizard, you must have access to a metric store used with Metrics Manager version 2.0 or later or you must create a database for a new metric store (p. 124).

Steps

1. Start Cognos Connection.

2. Click the **New metric package** button .

3. Type a name and description for the Metric Studio application to represent this metric package, and click **Next**.

4. Click **New data source**.

5. Type a name and description for the data source connection for the metric store that contains the content for this metric package, and click **Next**.
6. In the **Type** box, click the database type.
7. Select the isolation level, and click **Next**.
8. Specify the information required for your database type:
   - For a Microsoft SQL Server database, type the name of the database server and the database. Under **Signons**, select the **Password** and **Create a signon that the Everyone strategy can use** check boxes, and type the user ID and password of the user account with access to the database.
   - For an Oracle database, type the connection string. Select **User ID**, select the **Password** and **Create a signon that the Everyone strategy can use** check boxes, and type the user ID and password of the user account with access to the database.
   - For a DB2 database, type the name of the database, the connection string, and the collation sequence. Select **User ID**, select the **Password** and **Create a signon that the Everyone strategy can use** check boxes, and type the user ID and password of the user account with access to the database.

   Tip: To test whether the parameters are correct, click **Test**.
9. Click **Next** and then click **Finish**.
10. Click the new data source and click **Next**.
11. Click **Next** and follow the prompts to provide the information necessary to initialize the database. When you see the page that summarizes the data source details and the metric store settings, click **Initialize**.
12. Select **Open this package with Metric Studio after closing the wizard** and then click **Finish**.

Steps Using an Existing Metric Store

1. Start Cognos Connection.
2. Click the **New metric package** button .
3. Type the name and description for the Metric Studio application to represent this metric package and click **Next**.
4. Click **New data source**.
5. Type the name and description for the data source connection for the metric store that contains the content for this metric package, and click **Next**.
6. In the **Type** box, click the database type and click **Next**.
7. Specify the information required for your database type:

- For a Microsoft SQL Server database, type the name of the database server and the database. Under **Signons**, select the **Password** and **Create a signon that the Everyone group can use** check boxes, and type the user ID and password of the user account with access to the database.
- For an Oracle database, type the connection string. Under **User ID**, select the **Password** and **Create a signon that the Everyone group can use** check boxes, and type the user ID and password of the user account with access to the database.
- For a DB2 database, type the name of the database and the connection string. Select **User ID**, select the **Password** and **Create a signon that the Everyone group can use** check boxes, and type the user ID and password of the user account with access to the database.

Tip: To test whether the parameters are correct, click **Test**.

8. Click **Next**.
9. Select **Open this package with Metric Studio after closing the wizard** and then click **Finish**.

   Metric Studio opens and the new metric package is displayed in Cognos Connection.
10. Click the new data source and click **Next**.
11. Click **Upgrade**.

    The wizard updates the database schemas and other information.

For information about managing the metric store, see the *Administration and Security Guide*.

Configuring Framework Manager Computers

After you install Framework Manager on your Windows computer, you configure it so that it works in your reporting environment.

Some configuration tasks are optional. You perform them to change the default property values used by Framework Manager.

If you install Framework Manager on the same computer as the non-modeling components of Cognos 8, no configuration is required if you

- configure your Web server using the default virtual directories
- use the default ports
- use the default resources
- use the default cryptographic settings

If you upgraded from an older version of Framework Manager, you can use the same models and projects that you used with the older version. To upgrade existing projects, you must open them in the new version of Framework Manager.

If you install Framework Manager on a different computer from the non-modeling components of Cognos 8, you must do the following:

❑ Configure environment properties for Framework Manager computers.

- ❑ Configure a source control system.
- ❑ Upgrade Framework Manager projects, if required.

Configure Environment Properties for Framework Manager Computers

If you install Framework Manager on a different computer from the non-modeling components of Cognos 8, you must configure it to communicate with the other components.

We recommend that you install and configure Cognos 8 components before you configure Framework Manager. You must first install and configure Content Manager and then start the Cognos 8 service on at least one Content Manager computer before you configure Framework Manager. This ensures that the certificate authority service issues a certificate to the Framework Manager computer.

Important: If Cognos 8 was installed in more than one location, ensure that all URIs point to the correct version of Cognos 8. Framework Manager must be configured to use the same version of Cognos 8.

Installations with a Firewall

When the modeling tool is outside a network firewall that protects the Application Tier Components, communication issues with the dispatcher can arise. To avoid communication issues, you can install the modeling tool in the same architectural tier as the Application Tier Components or you can install and configure a gateway that is dedicated to modeling tool communications. For more information about the modeling tool and network firewalls, see "Firewall Considerations" (p. 32).

The steps in this topic describe how to configure the modeling tool computer. If you are using a gateway that is dedicated to the modeling tool, you must also configure the gateway computer (p. 171).

Prerequisites

Ensure that the Web server is configured and running (p. 132).

You must also set up the data sources (p. 138) before you configure Framework Manager.

Steps

1. On the computer where you installed Framework Manager, start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, in the **Gateway URI** box, type the appropriate value.
   - To use ISAPI, replace cognos.cgi with **cognosisapi.dll**.
   - To use an Apache Web server, type the following syntax:

     For Apache 1.3 module,

     http://host_name:port/cognos8/cgi-bin/mod_cognos.dll

     For Apache 2.0 module,

     http://host_name:port/cognos8/cgi-bin/mod2_cognos.dll

Note: Ensure that you configured your Apache Web Server (p. 231).

- To use a servlet gateway, type the following syntax:

  http[s]://host_name:port/context_root/servlet/Gateway

  where *context_root* is the value you assigned to the ServletGateway Web application when you deployed the ServletGateway application.

  Note: Ensure that you configured your Web server to support the servlet gateway (p. 233).

- If you are not using a Web server, to use the dispatcher as the gateway, type the following syntax:

  http[s]://*host_name:port*/p2pd/servlet/dispatch

4. Change the host name portion of the **Gateway URI** from localhost to either the IP address of the computer or the computer name.
5. Specify the value for the **Dispatcher URI for external applications**.
   - If your Web server is configured not to allow anonymous access, type the URI of the dispatcher, ensuring that you change the host name in the URI from localhost.
   - If your Web server supports chunked transfer encoding and Framework Manager is inside the firewall, type the URI of the dispatcher, ensuring that you change the host name in the URI from localhost.
   - If you are using a dedicated gateway for modeling tool communication, type the dispatcher URI.
6. In the **Explorer** window, under **Cryptography**, click **Cognos**, the default cryptographic provider.
7. Under the **Certificate Authority settings** property group, for the **Password** property, type the same password you configured on the default active Content Manager computer.
8. From the **File** menu, click **Save**.

Framework Manager is configured to communicate with the other components of Cognos 8. You can configure a source control system.

Configure a Source Control System

To help you manage, share, and secure different versions of your metadata, you can configure Framework Manager to use a source control system.

You must already have one of the following source control system clients set up on the same computer as Framework Manager:

- Component Software Concurrent Versions System
- Visual Source Safe

For more information about installing and setting up source control systems, see Repository Control in the Framework Manager *User Guide*.

Steps

1. Start Cognos Configuration.
2. In the **Explorer** window, under **Environment**, right-click **Source Control Systems** and click **New resource**, **Source Control System**.

   Source Control System is available on Windows computers that have Framework Manager installed and on Windows or UNIX computers that have Application Tier Components installed.
3. In the **Name** box, type a name for your source control system.
4. In the **Type** box, select a source control system from the list.
5. Click **OK**.
6. In the **Properties** window, for the **Source control system executable file (.exe) location** property, specify the file location and name of the .exe file.
   - For VSS, type **file_location\ss.exe**
   - For CVS, type ***file_location\cvs-version*.exe**

     where *version* is the CVS version number.
7. From the **File** menu, click **Save**.

You can now test your installation and configuration. You can also change default settings, if required. For example, you can change a port, configure SSL protocol, configure cryptographic settings, or change the Gateway URI to use an alternate gateway.

If you upgraded from an older version of Framework Manager, you can upgrade existing projects in the new version of Framework Manager.

Upgrade Framework Manager Projects

You can upgrade the metadata in an earlier version of a Framework Manager project by opening the project in the latest version of Framework Manager. A message appears indicating that the project was created using an older version of Framework Manager and asking if you want to specify a location for the backup file.

Before upgrading a project, we recommend that you do the following:

- Update any dependent projects or segments that you referenced in your project.

  For example, if your project links to a segment in a different project, you must upgrade the segment first. You can then upgrade the parent project.

  For more information, see the Framework Manager *User Guide*.
- Check out the project you want to upgrade using the third-party repository control.

  For more information, see the third-party vendor documentation.

- To upgrade a model that is located on a LAN, you must copy the model to a folder on a local machine. From your local machine, upgrade the model, and then copy the project back to the original LAN location.

Steps

1. Start Framework Manager.

   If the model schema version is older than the currently supported version, you may be prompted to specify a location for a backup of the project. If you click **Cancel**, Framework Manager will not open the project.

2. In the **Start** page, click **Open a project**.
3. Locate the project folder you want to open, and click the .cpf file.
4. Click **Open**.
5. If you are prompted for a location to store the backup, choose a location:
   - To save the backup model in the default location, click **No**.
   - To specify a different location, click **Yes** and browse to the location.
6. Click **OK**.

You must now republish your packages to a current version of the Application Tier Components server. For more information, see the Framework Manager *User Guide*.

To take a tour of Cognos 8, start Cognos Connection and select Quick Tour. For information about using different Cognos 8 components, see their documentation.

Configuring Transformer

If you install Cognos 8 Transformer on a different computer from the non-modeling components of Cognos 8, you must configure it to communicate with the other components. You may also want to make Transformer available for Transformer modelers to personally install on their computers.

The instructions in this topic are for the installer or administrator. If you are the Transformer modeler or business specialist who wants to download and use Transformer, see "Deploying Cognos 8 Transformer for Modelers" (p. 187).

If you install Transformer on a Windows Vista computer, and you plan to use the cogtr.xml.samples file as a template, you must update default preferences in the Transformer configuration file.

If you want to use Transformer models from Cognos Series 7 and you want to continue to use IQD data sources, you must add the locations of your Cognos Series 7 data sources to the Cognos Series 7 gateway file.

To configure the Transformer computers, do the following:

- ❑ Configure properties on the Transformer computers.
- ❑ Update default preferences in the Transformer configuration file, if required

- ❑ Add the locations of your Cognos Series 7 data sources to the Cognos Series 7 gateway file, if required

To make Transformer available for modelers to install, do the following:

- ❑ Create a network installation location for Transformer.
- ❑ Export configuration data for Transformer modelers.

Configure Cognos 8 Transformer Computers

You must configure Cognos 8 Transformer to communicate with the other Cognos 8 components.

The instructions in this topic are for the installer or administrator. If you are the Transformer modeler or business specialist who wants to download and use Transformer, see "Deploying Cognos 8 Transformer for Modelers" (p. 187).

If you install Cognos 8 Transformer on the same computer as the non-modeling components of Cognos 8, no configuration is required if you

- configure your Web server using the default virtual directories
- use the default ports
- use the default resources
- use the default cryptographic settings

You can upgrade models from Series 7.x versions of Transformer if you have saved them as MDL files.

You can continue to use PowerCubes built with Series 7.3 and higher versions of Transformer in Cognos 8. However, to use Cognos 8 authentication providers, you must upgrade the PowerCubes.

To upgrade PowerCubes to Cognos 8 PowerCubes, you must:

- open the Series 7.x Transformer model MDL file in Cognos 8 Transformer
- rebuild the PowerCube in the Cognos 8 Transformer

For more information about upgrading Series 7 PowerCubes, see "Upgrading Transformer Models and PowerCubes" (p. 83).

Important: If Cognos 8 was installed in more than one location, ensure that all URIs point to the correct version of Cognos 8. Transformer must be configured to use the same version of Cognos 8.

Installations with a Firewall

When the modeling tool is outside a network firewall that protects the Application Tier Components, communication issues with the dispatcher can arise. To avoid communication issues, you can install the modeling tool in the same architectural tier as the Application Tier Components or you can install and configure a gateway that is dedicated to modeling tool communications. For more information about the modeling tool and network firewalls, see "Firewall Considerations" (p. 35).

The steps in this topic describe how to configure the modeling tool computer. If you are using a gateway that is dedicated to the modeling tool, you must also configure the gateway computer (p. 171).

Prerequisites

We recommend that you install and configure Cognos 8 components before you configure Cognos 8 Transformer. You must first install and configure Content Manager and then start the Cognos 8 service on at least one Content Manager computer before you configure Cognos 8 Transformer. This ensures that the certificate authority service issues a certificate to the Cognos 8 Transformer computer.

Ensure that the Web server is configured and running (p. 132).

To support the use of Cognos 8 data sources (including packages and reports) in Transformer, ensure that the database client is installed on the Transformer computer (p. 127).

Steps

1. On the computer where you installed Cognos 8 Transformer, start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, in the **Gateway URI** box, type the appropriate value.
   - To use ISAPI, replace cognos.cgi with **cognosisapi.dll**.
   - To use an Apache Web server, type the following syntax:

     For Apache 1.3 module,

     http://*host_name:port*/cognos8/cgi-bin/mod_cognos.dll

     For Apache 2.0 module,

     http://*host_name:port*/cognos8/cgi-bin/mod2_cognos.dll

     Note: Ensure that you configured your Apache Web Server (p. 231).
   - To use a servlet gateway, type the following syntax:

     http[s]://*host_name:port/context_root*/servlet/Gateway

     where *context_root* is the value you assigned to the ServletGateway Web application when you deployed the ServletGateway application.

     Note: Ensure that you configured your Web server to support the servlet gateway (p. 233).
   - If you are not using a Web server, to use the dispatcher as the gateway, type the following syntax:

     http[s]://*host_name:port*/p2pd/servlet/dispatch
4. Change the host name portion of the **Gateway URI** from localhost to either the IP address of the computer or the computer name.
5. Specify the value for the **Dispatcher URI for external applications**.

- If your Web server is configured not to allow anonymous access, type the URI of the dispatcher, ensuring that you change the host name in the URI from localhost.
- If your Web server supports chunked transfer encoding and Cognos 8 Transformer is inside the firewall, type the URI of the dispatcher, ensuring that you change the host name in the URI from localhost.
- If you are using a dedicated gateway for modeling tool communication, type the dispatcher URI.

6. In the **Explorer** window, under **Cryptography**, click **Cognos**, the default cryptographic provider.
7. Under the **Certificate Authority settings** property group, for the **Password** property, type the same password you configured on the default active Content Manager computer.
8. From the **File** menu, click **Save**.

   Cognos 8 Transformer is configured to communicate with the other components of Cognos 8.
9. If you installed Transformer on a Windows Vista computer, or if any Cognos 8 BI component is installed on a Windows Vista computer, update your file location properties:
   - Log on as an administrator.
   - In the *c8_location*\configuration directory, open cogtr.xml.sample in a text editor.
   - Locate all values that use a relative path, "..*directory*".
   - Replace the relative path element, "..", with the same environment variable and root directory as you use for file locations on the other Cognos 8 computers.
   - Save the file as cogtr.xml.
   - In the *c8_location*\CS7Gateways\bin directory, open cs7g.ini in a text editor.
   - Add the locations for your Cognos Series 7 data sources to the file.
   - Save the file.

   Changes are applied the next time you open Transformer.

Update Default Preferences for Windows Vista

With security enhancements in Windows Vista, Microsoft changed the structure of user directories. If you want to use the cogtr.xml.samples file as a template, you must edit the default preferences settings. If you want all users to have the same default directories, you must change the default preferences to a common location to which users have access. If you want users to have the Windows Vista directories, you can delete the default preferences for the directories.

The instructions in this topic are for the installer or administrator. If you are the Transformer modeler or business specialist who wants to download and use Transformer, see "Deploying Cognos 8 Transformer for Modelers" (p. 187).

Steps

1. Log on as the administrator.
2. In the *c8_location*\configuration directory, open cogtr.xml.sample in a text editor in elevated mode by right-clicking on the text editor and selecting **Run as Administrator**.
3. If you want all users to have the same default directories, change the directories to a location to which all users have read and write access.

   The directories to change are as follows:

   - `<Preference Name="CubeSaveDirectory" Type="string" Value="..\temp"/>`
   - `<Preference Name="DataSourceDirectory" Type="string" Value="..\temp"/>`
   - `<Preference Name="DataWorkDirectory" Type="string" Value="..\temp"/>`
   - `<Preference Name="LogFileDirectory" Type="string" Value="..\logs"/>`
   - `<Preference Name="ModelSaveDirectory" Type="string" Value="..\temp"/>`
   - `<Preference Name="ModelWorkDirectory" Type="string" Value="..\temp"/>`
4. If you want users to have the Windows Vista default directories, delete the preferences specified in step 3 from the file.

   The Windows Vista default directories for Transformer are

   - CubeSaveDirectory

     Documents\Transformer\PowerCubes
   - DataSourceDirectory

     In Cognos Configuration, under **Environment**, **Data files location** property
   - DataWorkDirectory

     In Cognos Configuration, under **Environment**, **Temporary files location** property
   - LogFileDirectory

     Documents\Transformer\Logs
   - ModelSaveDirectory

     Documents\Transformer\Models
   - ModelWorkDirectory

     In Cognos Configuration, under **Environment**, **Temporary files location** property
5. Change other settings as required.
6. Save the file as cogtr.xml.

The changes are applied the next time you open Transformer.

Add Cognos Series 7 Data Sources to Transformer

If you plan to use Transformer models and data sources from Cognos Series 7, you must add the location of your Cognos Series 7 data sources to the Transformer gateway file.

The instructions in this topic are for the installer or administrator. If you are the Transformer modeler or business specialist who wants to download and use Transformer, see "Deploying Cognos 8 Transformer for Modelers" (p. 187).

Steps

1. Log on as the administrator.
2. In the c8_location\CS7Gateways\bin directory, open cs7g.ini in a text editor.

   On Windows Vista, open it in elevated mode by right-clicking on the text editor and selecting **Run as Administrator**.
3. Add the locations for your Cognos Series 7 data sources to the file.
4. Save the file.

   The changes are applied the next time you open Transformer.

Create a Network Installation Location for Transformer Modelers

Your organization may have specialized business or power users who want to build PowerCubes that are modeled on a combination of corporate and personal data sources. These users may want to do their own analysis of the data for their line of business or a small group of users. An installer or administrator can download an executable file to a Web or LAN location, where modelers can run the file to launch the Cognos 8 Transformer installation wizard.

The instructions in this topic are for the installer or administrator. If you are the Transformer modeler or business specialist who wants to download and use Transformer, see "Deploying Cognos 8 Transformer for Modelers" (p. 187).

Before you make the installation file available to Transformer modelers, other resources and permissions must be set up:

- Database client software is installed, or available for modelers to install, on the Transformer computers that are used to access Cognos 8 data sources or Cognos Series 7 IQD data sources.
- Modelers must have privileges to create a data source in Cognos Administration.

  Modelers do not need direct access to Cognos Administration. They can create and update data sources by using Transformer or command line tools. You can provide modelers with a secured folder in Cognos Connection in which to publish PowerCube packages.
- Modelers must have access to a location in which to store the PowerCube after building it.

  This location must also be accessible to the Cognos 8 service and can be a secured share on a LAN.

- Modelers may require special privileges to remotely run the Cognos 8 PowerCube Connection utility, which is located on the Cognos 8 server. For more information, see the topic about updating published PowerCubes and PowerCube connections in the Transformer *User Guide*.
- To build PowerCubes on a specific Transformer server, modelers should have FTP privileges to transfer models and execute privileges to build cubes on that server.

  Modelers can transfer models and execute cube builds using scripts. Modelers can also use automated methods to build PowerCubes. For more information, see the *Administration and Security Guide*.

Steps

1. Insert the CD for Cognos 8 Transformer modeling product.
2. If the **Welcome** page of the installation wizard appears, exit the wizard.
3. On the CD, locate the c8transformerinstall.exe file.
4. Copy the file to a secure location to which your Transformer modelers have access.

Export Configuration Data for Transformer Modelers

If you want to make the Transformer installation file available to Transformer modelers, the modelers will need the dispatcher and encryption settings to configure Transformer on their local computer. You can export the configuration from one Transformer computer for use with all other Transformer computers. The modelers can copy the exported configuration file to their Transformer installation directory and then run the command to configure the Transformer computer silently.

The instructions in this topic are for the installer or administrator. If you are the Transformer modeler or business specialist who wants to download and use Transformer, see "Deploying Cognos 8 Transformer for Modelers" (p. 187).

If you updated the coglocale, cogtr.xml, or cs7g.ini files on the Transformer computer, you must copy these files to the Web or LAN location so that Transformer modelers can download them to their computer.

To export the configuration, the source computer must have the same Cognos 8 components as the Transformer modeler computers (p. 181). If some modelers will be installing on Windows Vista, you must create an export file from a Windows Vista computer. We suggest creating separate folders on the Web or LAN location for Windows and Windows Vista.

Steps to Export the Transformer Computer Configuration

1. In Cognos Configuration, from the **File** menu, click **Export as**.
2. If you want to export the current configuration to a different folder, in the **Look in** box, locate and open the folder.

   Ensure that the folder is protected from unauthorized or inappropriate access.
3. In the **File name** box, type a name for the configuration file.
4. Click **Save**.

5. Rename the exported file to cogstartup.xml.
6. Copy the exported cogstartup.xml file from the source computer to the same Web or LAN location as the Transformer installation file.
7. If you changed the global configuration on the source computer, copy the coglocale.xml file from the source computer to the same Web or LAN location as the Transformer installation file.

   The default location of the coglocale.xml file is *c8_location*\configuration.

Steps to Download Transformer Configuration Files

1. If you updated the cogtr.xml, copy it from the *c8_location*\configuration directory to the same Web or LAN location as the Transformer installation file.
2. If you updated the cs7g.ini file, copy it from the *c8_location*\CS7Gateways\bin directory to the same Web or LAN location as the Transformer installation file.

Deploying Cognos 8 Transformer for Modelers

If you are the business specialist or Transformer modeler, you must now deploy Transformer so that you can build PowerCubes and publish them to selected users or groups.

If you have not completed the installation, follow the steps to install Transformer. To configure Transformer so that it can communicate with the Cognos 8 dispatcher, follow the steps to configure Transformer.

If Cognos Connection is secured, you must have privileges to create data sources and publish packages in Cognos Connection.

You can upgrade models from Series 7.x versions of Transformer if you have saved them as MDL files.

You can continue to use PowerCubes built with Series 7.3 and higher versions of Transformer in Cognos 8. However, to use Cognos 8 authentication providers, you must upgrade the PowerCubes. After upgrading, the PowerCubes are no longer compatible with Series 7 Transformer.

To upgrade PowerCubes to Cognos 8 PowerCubes, you must:

- open the Series 7.x Transformer model MDL file in Cognos 8 Transformer
- rebuild the PowerCube in the Cognos 8 Transformer

For more information, see "Upgrading Transformer Models and PowerCubes" (p. 83).

To support the use of Cognos 8 data sources (including packages and reports) in Transformer, ensure that the database client is installed on the Transformer computer (p. 127).

Steps to Install Transformer

1. From the Web or LAN location that the administrator provided, run the c8transformerinstall.exe file.

The contents are expanded to the Documents and Settings*username*\Local settings\Temp directory and then the Transformer installation wizard opens.

2. Follow the directions in the installation wizard and copy the required files to your computer.

   Tip: The Series 7 IQD Bridge component is not supported on Linux and HP-UX Itanium.

3. In the **Finish** page of the wizard, select **View the Readme** and then click **Finish**.

   Tip: For character-mode installations on UNIX and Linux, close the readme text file by pressing Ctrl + C or Q.

4. Create a MANPATH environment variable and configure it to point to the cogtr.1 file in the *Transformer_location*/webcontent/documentation/en directory.

   The cogtr.1 file provides the syntax for UNIX command line options that are supported by Cognos 8 Transformer. The man page is accessible in UNIX by typing **man**.

Steps to Configure Transformer

1. Go to the same Web or LAN location as the Transformer installation file.
2. If any .xml files are present, copy them to the *Transformer_location*\configuration directory, where *Transformer_location* is the directory where you installed Transformer.

   The default location is C:\Program Files\Cognos\c8.

3. If an .ini file is present, copy it to the *Transformer_location*\CS7Gateways\bin directory.
4. Go to the *Transformer_location*\bin directory.
5. Type the configuration command:

   ./cogconfig.bat -s

   Cognos Configuration applies the configuration settings specified in the local copy of cogstartup.xml, encrypts credentials, generates digital certificates, and starts the Cognos 8 service.

6. To test Cognos 8 Transformer, from the **Start** menu, click **Programs**, **Cognos 8**,**Transformer**.

   If you see the **Transformer** window, your installation is working.

7. After Transformer is intalled and running successfully, delete the installation files that were extracted from the installation file.

Configure Metric Designer

If you install Metric Designer on the same computer as other Cognos 8 components, no configuration is required. If you install Metric Designer on a different computer from other Cognos 8 components, you must configure environment properties for Metric Designer computers.

If you upgraded from Metrics Manager version 2.0 or later, you can use the same extracts and projects that you used with the older version. To upgrade existing projects, you must open them in the new version of Metric Designer and redefine the data source connections and other references.

Before you configure Metric Designer, other Cognos 8 components must be installed and configured, and Metric Designer must be installed.

Configure Environment Properties for Metric Designer Computers

If you install Metric Designer on a different computer from other Cognos 8 components, you must configure it to communicate with the computers where the gateway and Content Manager are installed.

We recommend that you install and configure other Cognos 8 components before you configure Metric Designer. You must first install and configure Content Manager and then start the Cognos 8 service on at least one Content Manager computer before you configure Metric Designer. This ensures that the certificate authority service issues a certificate to the Metric Designer computer.

Before you configure Metric Designer, ensure that the Web server is configured and running, and the Cognos 8 service is running.

If you are using an Apache Web server, ensure that you configure it first (p. 231).

Installations with a Firewall

When the modeling tool is outside a network firewall that protects the Application Tier Components, communication issues with the dispatcher can arise. To avoid communication issues, you can install the modeling tool in the same architectural tier as the Application Tier Components or you can install and configure a gateway that is dedicated to modeling tool communications. For more information about the modeling tool and network firewalls, see "Firewall Considerations" (p. 32).

The steps in this topic describe how to configure the modeling tool computer. If you are using a gateway that is dedicated to the modeling tool, you must also configure the gateway computer (p. 171).

Steps

1. On the computer where you installed Metric Designer, start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, in the **Gateway URI** box, type the appropriate value:
   - Change the host name portion of the **Gateway URI** from localhost to either the IP address of the computer or the computer name.
   - To use ISAPI, replace cognos.cgi with **cognosisapi.dll**.
   - To use apache_mod, type the following syntax:

     http://*host_name:port*/cognos8/cgi-bin/*module*

     where *module* is as follows:

Operating system	Apache 1.3 module	Apache 2.0 module
Windows	mod_cognos.dll	mod2_cognos.dll

Operating system	Apache 1.3 module	Apache 2.0 module
Solaris or AIX	mod_cognos.so	mod2_cognos.so
HP-UX PA-RISC	mod_cognos.sl	mod2_cognos.sl
HP-UX IA	(not supported)	mod2_cognos.so

4. Specify the value for the **Dispatcher URI for external applications**.
   - If your Web server is configured not to allow anonymous access, type the URI of the dispatcher, ensuring that you change the host name in the URI from localhost.
   - If your Web server supports chunked transfer encoding and Metric Designer is inside the firewall, type the URI of the dispatcher, ensuring that you change the host name in the URI from localhost.
   - If you are using a dedicated gateway for modeling tool communication, type the dispatcher URI.
5. From the **File** menu, click **Save**.

Metric Designer is configured to communicate with other Cognos 8 components.

Upgrade Metric Designer Projects

You can upgrade the metadata in an earlier version of a Metrics Designer project by opening the project in the current version of Metric Designer. A message appears indicating that the project was created using an earlier version of Metrics Designer and asking if you want to specify a location for the backup file.

Before upgrading a project with a model that is located on a LAN, you must copy the model to a folder on a local machine. From your local machine, upgrade the model, and then copy the project back to the original LAN location.

Steps

1. Start Metric Designer.
2. In the **Start** page, click **Open a Project**.
3. Locate the project folder you want to open, and click the .cpf file.
4. Click **Open**.
5. If you are prompted for a location to store the backup, choose a location:
   - To save the backup model in the default location, click **No**.
   - To specify a different location, click **Yes** and browse to the location.

You are prompted to back up the project if the model schema version is older than the currently supported version. If you click **Cancel**, Metric Designer will not open the project.

6. If the metric package or data source connection associated with the project no longer exists, you are prompted to choose an existing metric package or data source connection to be used.
7. Click **OK**.

Start the Cognos 8 Services

To register the Cognos 8 service so that users can access it through Cognos Connection, you must start the services. Before you start the services, test the configuration by using the test feature in Cognos Configuration.

Before you can use Framework Manager, Cognos 8 Transformer, or Metric Designer, you must start the Cognos 8 service. On Windows, the Cognos 8 service is configured to start automatically by default. On UNIX and Linux, to start the Cognos 8 process automatically, you must configure the process as a daemon. For more information, see your operating system documentation.

You must install and configure both the server components of Cognos 8 and Framework Manager before you can use Cognos 8 for reporting.

Note: Cognos 8 cannot access any reporting data unless the data is first packaged in and published from Framework Manager.

Steps

1. Start Cognos Configuration.
2. Ensure that you save your configuration, otherwise you cannot start the Cognos 8 service.

   If you are upgrading, a message appears indicating that configuration files were detected and upgraded to the new version.
3. From the **Actions** menu, click **Test**.

   Cognos Configuration checks the CSK availability, tests the namespace configuration, and tests the connections to the content store and logging database.

   If you are using the notification database and the mail server, they are tested as well.

   Tip: If **Test** is not available for selection, in the **Explorer** window, click **Local Configuration**.
4. If the test fails, reconfigure the affected properties and then test again.

   You can test individual services by right-clicking the service in the **Explorer** panel and selecting **Test**.

   Do not start the service until all tests pass.
5. From the **Actions** menu, click **Start**.

   It may take a few minutes for the Cognos 8 service to start.

This action starts all installed services that are not running. If you want to start a particular service, select the service node in the **Explorer** window and then click **Start** from the **Actions** menu.

Test the Installation and Configuration

You can test your configuration settings by running the test feature as you configure Cognos 8. After you have completed the configuration and started the services, you can test the installation by opening Cognos Connection. If you installed Framework Manager, Cognos 8 Transformer, or Metric Designer, you can test it by starting the application and creating a project.

If you installed Metric Studio and you have created a package, you have already tested your installation and configuration. You can create a metric package only if Metric Studio is installed and configured properly.

Steps for Content Manager or Application Tier Components Computer

1. Open a Web browser.
2. Test the availability of the dispatcher by typing

   http://*ContentManagerComputer_name:port*/p2pd/servlet

   If the response includes the string State: Running, the dispatcher is available.

Steps for Gateway Computer

1. Open a Web browser.
2. Test the availability of the dispatcher by typing

   http://*ContentManagerComputer_name:port*/p2pd/servlet

   If the response includes the string State: Running, the dispatcher is available.
3. Open Cognos Connection by typing one the following, where cognos8 is the virtual directory you created when you configured the Web server.
   - For the CGI gateway:

     http://*GatewayComputer_name:port*/cognos8
   - For an ISAPI gateway:

     http://*GatewayComputer_name:port*/cognos8/isapi
   - For Apache Connector on Windows:

     http://*GatewayComputer_name:port*/cognos8/cgi-bin/mod_cognos.dll
   - For Apache Connector on Solaris or AIX:

     http://*GatewayComputer_name:port*/cognos8/cgi-bin/mod_cognos.so
   - For Apache Connector on HP-UX PA-RISC:

     http://*GatewayComputer_name:port*/cognos8/cgi-bin/mod_cognos.sl

- For Apache Connector on HP-UX IA:

  http://*GatewayComputer_name:port*/cognos8/cgi-bin/mod2_cognos.so

- For a gateway servlet:

  http://*GatewayComputer_name:port*/context_root/servlet/ Gateway

It may take a few minutes for the Web page to open. If you see the **Welcome** page of Cognos Connection, your installation is working.

Step for Framework Manager

- To start Framework Manager, from the **Start** menu, click **Programs**, **Cognos 8**, **Framework Manager**.

  You may be prompted to upgrade if the model schema version is older than the currently supported version.

  If you see the **Welcome** page of Framework Manager, your installation is working.

Step for Cognos 8 Transformer

- To start Cognos 8 Transformer, from the **Start** menu, click **Programs**, **Cognos 8**,**Transformer**.

  To start Cognos 8 Transformer manually, double-click the following file in the *c8_location*\bin directory:

  - For Windows, cogtr.exe
  - For UNIX or Linux, cogtr.sh

  If you see the **Transformer** window, your installation is working.

Step for Metric Designer

- To start Metric Designer, from the **Start** menu, click **Programs**, **Cognos 8**, **Metric Designer**.

  If you see the **Welcome** page of Metric Designer, your installation is working.

Changing Default Configuration Settings

When you install Cognos 8 components, the installation uses default configuration settings. If you have any reason not to use these default values, such as a port is being used by another process, use Cognos Configuration to change the value.

If you change the value of a property, you must save the configuration and then restart the Cognos 8 service to apply the new settings to your computer.

For distributed installations, ensure that you configured all computers where you installed Content Manager before you change default configuration settings on other Cognos computers. For example you can

- change the default user and password for Cognos Content Database

- change a URI
- configure cryptographic settings
- configure Cognos 8 components to use Cognos Application Firewall
- configure temporary file properties
- configure the gateway to use a namespace
- enable and disable services
- specify the amount of resources the Cognos 8 service uses
- configure fonts
- change the default font for reports
- save report output to a file system
- change the location of map charts for Report Studio

After you change the default behavior of Cognos 8 to better suit your Cognos environment, you can configure Portal Services, configure an authentication provider, or test the installation and configuration.

For Cognos 8, you can install and configure Framework Manager. For Metric Studio, you can install and configure Metric Designer.

Change Default User and Password for Cognos Content Database

If you install Cognos Content Database, the default database that is created is given a user ID and password. We recommend that you change this user ID and password.

Administration tasks for Cognos Content Database are performed using a utility named ij. For information about this utility, see the Apache Derby documentation. The documentation is available in the *c8_location*\derby10.1.2.1\docs directory where you installed Cognos Content Database.

Steps to Change the Default User Password

1. On the computer where you installed Cognos Content Database, go to the *c8_location*\derby10.1.2.1\bin directory.
2. Start the ij utility using the ij.bat or ij.ksh script file.

   The ij utility is a command line utility for creating and managing Cognos Content Database.
3. Connect to the default database by typing the following ij utility command:

   connect 'jdbc:derby://localhost:1527/cm;user=cognos;password=cognos';

   If you changed the port number from the default 1527, use the correct port number for your Cognos Content Database.

   The default database is named cm. The database name is case sensitive.
4. Change the default password for the cognos user by typing the following ij utility command:

CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.cognos', 'NewPassword');

The new password must be used for the next connection to the database.

5. Close the ij utility by typing the following command:

   disconnect;

Steps to Create a New User and Password

1. On the computer where you installed Cognos Content Database, go to the *c8_location*\derby10.1.2.1\bin directory.
2. Start the ij utility using the ij.bat or ij.ksh script file.
3. Connect to the default database by typing the following ij utility command:

   connect 'jdbc:derby://localhost:1527/cm;user=cognos;password=cognos';

   If you changed the port number from the default 1527, use the correct port number for your Cognos Content Database.

   The default database is named cm. The database name is case sensitive.
4. Create a new user by typing the following ij utility command:

   CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.NewUser', 'NewUserPassword');
5. Give the new user full access to the database by typing the following ij utility command:

   CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY ('derby.database.fullAccessUsers',’cognos, NewUser');

   The property that you are changing, the list of users, is a comma-delimited field. In this step, you are including the new user in the list of users with full access. The default user, cognos, is still part of the list of users with full access. You can remove the cognos user.
6. Close the ij utility by typing the following command:

   disconnect;

Steps to Remove a User

1. On the computer where you installed Cognos Content Database, go to the *c8_location*\derby10.1.2.1\bin directory.
2. Start the ij utility using the ij.bat or ij.ksh script file.
3. Connect to the default database by typing the following ij utility command:

   connect 'jdbc:derby://localhost:1527/cm;user=NewUser; password=NewUserPassword';
4. Choose the kind of user that you want to remove:
   - To remove a user from the list of users with full access, type the following ij utility command:

CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY ('derby.database.fullAccessUsers', 'NewUser');

You omit the user name from the list of users with full access. For example, the above command removes the default cognos user and keeps the new user that you just created.

- To remove a user from the database, type the following ij utility command and omit the user password:

  CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.cognos', '');

  This command removes the password for the default cognos user, which also removes the user from the database.

5. Close the ij utility by typing the following command:

   disconnect;

Change a URI

You can change certain elements in a URI depending on your environment. A Cognos URI contains the following elements:

- For a Content Manager URI, Dispatcher URI for external applications, or dispatcher URI

  protocol://host_name_or_IP:port/context_root/alias_path

- For a Gateway URI or a Web content URI

  protocol://host_name_or_IP:port/virtual_directory/gateway_application

  OR

  protocol://host_name_or_IP:port/context_root/alias_path

Element	Examples	Description
protocol	http or https	Specifies the protocol used to request and transmit information, either Hyper Text Transfer Protocol or Hyper Text Transfer Protocol (Secure).

Element	Examples	Description
host name or IP	localhost or 192.168.0.1	Specifies the identity of the host on the network. You can use an IP address, a computer name, or a fully qualified domain name. In a distributed installation, you must change the localhost element of a URI. In a mixed environment of UNIX and Windows servers, ensure that host names can be resolved to IP addresses by all servers in the environment.
port	9300 or 80	Specifies the port on which the host system listens for requests. The default port for Tomcat is 9300. The default port for a Web server is 80.
context root	p2pd	Used by Tomcat or an application server to determine the context of the application so that the request can be routed to the correct Web application for processing.

Element	Examples	Description
alias path	servlet/dispatch	Used by the application server to route a request to the correct component within a Web application. The alias path must not be modified or Cognos 8 components will not function properly.
virtual directory	cognos8/	Used by the Web server to map a virtual directory or alias to a physical location. For example, in the default Gateway URI of http://localhost:80/cognos8/cgi-bin/cognos.cgi, the virtual directory is cognos8/cgi-bin.
gateway application	cognos.cgi	Specifies the name of the Cognos gateway application that is used. For example, if you are accessing Cognos 8 components using a Common Gateway Interface (CGI), then the default gateway application would be cognos.cgi.

Steps

1. Start Cognos Configuration.
2. In the **Explorer** window click the appropriate group or component:

- To change an element for the dispatcher, click **Environment**.
- To change an element for the local log server, under **Environment**, click **Logging**.

3. In the **Properties** window, click the **Value** box next to the URI property that you want to change.
4. Select the element and type the new information.

   Tip: To change the port used by the local dispatcher, change the value of the Internal dispatcher URI property. Because the change affects all the URIs that are based on the local dispatcher, you must change the URIs of all local components.

   Tip: If you change the dispatcher port in the dispatcher URI, ensure that you specify the new port number when you configure remote computers that use the dispatcher, Content Manager, or SDK services on this system.
5. From the **File** menu, click **Save**.

Configure Cryptographic Settings

Cognos 8 components require a cryptographic provider; otherwise they will not run. If you delete the default cryptographic provider, you must configure another provider to replace it.

You can configure cryptographic provider settings, including the following:

- advanced algorithms

  These include signing and digest algorithms.
- common symmetric key store (CSK) properties

  The CSK is used by Cognos 8 to encrypt and decrypt data.
- signing key store properties

  The signing key pair includes the private key used to generate the digital signature and the public key used to verify authenticity.
- encryption key store properties

  The encryption key pair includes the private key used to encrypt data and the public key used to decrypt data.

The default cryptographic provider uses keys up to 56 bits in length for data encryption and secure sockets layer (SSL) protocol. You can configure other cryptographic providers which use key sizes greater than 56 bits, such as the Enhanced Encryption Module for OpenSSL or the Enhanced Encryption Module for Entrust, available from Cognos. For more information, see the *Enhanced Encryption Module for OpenSSL Installation and Configuration Guide* or the *Enhanced Encryption Module for Entrust Installation and Configuration Guide*.

Important: In a distributed installation, Cognos computers communicate with Content Manager to establish trust and obtain some cryptographic keys from Content Manager. If you change the cryptographic keys in Content Manager, such as by changing application servers or reinstalling Content Manager, you must delete the cryptographic keys on the other Cognos computers. You must then save the configuration on each computer so that they obtain the new cryptographic keys

from Content Manager. In addition, all Cognos 8 components in a distributed installation must be configured with the same cryptographic provider settings.

Also, in a distributed environment, the symmetric key should only be stored on computers where Content Manager has been installed.

Steps for Cryptographic Settings

1. Start Cognos Configuration.
2. In the **Explorer** window, under **Security**, click **Cryptography**.
3. In the **Properties** window, change the default values by clicking the **Value** box and then selecting the appropriate value:
   - On computers that do not contain Content Manager, if you do not want to store the CSKs locally, under **CSK settings**, change **Store symmetric key locally** to **False**.

     When **Store symmetric key locally** is **False**, the key is retrieved from Content Manager when required. The **Common symmetric key store location** property is ignored.
   - If you want the computers at both ends of a transmission to prove their identity, under **SSL Settings**, change **Use mutual authentication** to **True**.

     We recommend that you do not change the **Use confidentiality** setting.
   - If you want to change the digest algorithm, for the **Digest algorithm** property, select another value.
4. From the **File** menu, click **Save**.
5. Test the cryptographic provider on a gateway computer only. In the **Explorer** window, right-click **Cryptography** and click **Test**.

   Cognos 8 components check the availability of the symmetric key.

After you configure the cryptographic provider, passwords in your configuration and any data you create are encrypted.

Steps for Cryptographic Provider

1. Start Cognos Configuration.
2. In the **Explorer** window, under **Security**, **Cryptography**, click **Cognos**.
   - If you want to change the location of the signing keys, under **Signing key settings**, change the **Signing key store location** property to the new location.
   - If you want to change the location of the encryption keys, under **Encryption key settings**, change **Encryption key store location** to the new location.
   - If you want to use a third-party certificate authority, under **Certificate Authority settings**, change **Use third party CA** to **True**.

     You must also ensure that you use the same values for the -k parameter as you used for the **Signing key store location** and **Encryption key store location** properties.

For more information, see "Configuring Cognos 8 Components to Use a Third-party Certificate Authority" (p. 317).

Important: The **Confidentiality algorithm** value determines how data is encrypted by Cognos 8 components. For example, database passwords entered in Cognos Configuration are encrypted when you save the configuration. The algorithm selected when the data is encrypted must also be available for the data to be decrypted at a later date.

The availability of confidentiality algorithms can change if there are changes to your environment. For example, if your Java Runtime Environment (JRE) has changed or if you have installed third-party cryptographic software on the computer. If you have made changes to a computer, such as upgraded the JRE or installed software that has upgraded the JRE, this may affect the availability of confidentiality algorithms. You must ensure that the **Confidentiality algorithm** that was selected when the data was encrypted is also available when you want to access the data.

3. From the **File** menu, click **Save**.

If you use a third-party Certificate Authority (CA) server, you must now configure Cognos 8 components to use the CA.

Configure Cognos 8 Components to Use Cognos Application Firewall

Cognos Application Firewall analyzes and validates HTTP and XML requests before they are processed by Cognos servers. Cognos Application Firewall may modify these HTTP and XML requests.

Cognos Application Firewall protects Cognos Web products from malicious data. The most common forms of malicious data are buffer overflows and cross-site scripting (XSS) attacks, either through script injection in valid pages or redirection to another Web site.

Using Cognos Configuration, you can change settings for third-party XSS tool support, and you can add host and domain names to the Cognos list of valid names.

You can track firewall activity by checking the log file, which contains rejected requests. By default, log messages are stored in the *c8_location*\logs\cogserver.log file.

Important: All CAF settings must be the same for all computers where Cognos 8 Application Tier Components are installed within a distributed environment. For example, if CAF is disabled on some computers and enabled on others, unexpected behavior and product errors may result.

Steps

1. On each computer where Cognos 8 Application Tier Components have been installed, start Cognos Configuration.
2. In the **Explorer** window, under **Security,** click **Cognos Application Firewall**.
3. In the **Properties** window, for the **Enable CAF validation** property, set the appropriate values.

   By default, Cognos Application Firewall is enabled.

Important: The Cognos Application Firewall is an essential component of Cognos security, helping to provide protection against penetration vulnerabilities. Disabling the Cognos Application Firewall will remove this protection. Under normal circumstances we recommend that you not disable the Cognos Application Firewall.

4. If you are using a third-party XSS tool that checks for specific characters in GET request parameters, in the **Properties** window, do the following:
   - For the **Is third party XSS checking enabled** property, change the value to **True**.
   - For the **Third party XSS characters** property, add any additional characters that are prohibited by the third-party XSS tool. The default characters are >, <, and '.
5. Add host and domain names to the Cognos list of valid names:
   - For the **Valid domains and hosts** property, click the value and then click the edit button.
   - In the **Value - Valid domains or hosts** dialog box, click **Add**.

     You must include the domains from all hyperlinks that are added in Cognos Connection. For more information, see the topic about creating a URL in the *Administration and Security Guide*.

     Tip: If you are using drill-through from Cognos Series 7 to reports in Cognos 8, add the hostnames of the Cognos Series 7 gateway servers to the list.
   - In the blank row of the table, click and then type the host or domain name.
   - Repeat the previous two bulleted steps for each name to be added.
   - Click **OK**.

   Cognos Application Firewall validates domain and host names to protect URLs that are created. By default, Cognos Application Firewall considers domain names derived from the environment configuration properties to be safe domain names. Adding names to the list of valid names and hosts is useful when you need to redirect requests to non-Cognos computers using the Back or Cancel functions or when using drill-through to different Cognos product installations.
6. Save the configuration.
7. Restart the services.

Configure Temporary File Properties

You can change the location where Cognos 8 components store recently viewed reports, and you can choose to encrypt their content. By default, Cognos 8 components store temporary files in the *c8_location*\temp directory and the files are not encrypted.

We recommend that all access be denied to the temp directory, except for the service account used to start the Cognos 8 service. Read and write permissions are required for the service account.

Steps

1. Start Cognos Configuration.

2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, for the **Temporary files location** property, specify the new location.
4. If you require the content of temporary files to be encrypted, set the **Encrypt temporary files** property to **True**.
5. Ensure that the user account under which Cognos 8 components run have the appropriate privileges to the temporary files location. For example:
   - on Windows, full control privileges
   - on UNIX or Linux, read-write privileges

Configure the Gateway to Use a Namespace

If Cognos 8 components use multiple namespaces or if anonymous access is enabled and Cognos 8 components use one namespace, you can configure the gateway to connect to one namespace. Users logged onto the Web server where the gateway is located are not prompted to choose an authentication source.

For example, if you have two Web servers, you can configure each Web server to use a different namespace.

Steps

1. On the computer where the gateway is located, start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, in the **Value** box next to the **Gateway namespace** property, type the Namespace ID of the namespace you want to use.
4. From the **File** menu, click **Save**.
5. Restart your Web server.

Enable and Disable Services

In a distributed installation, you can send certain types of requests to specific computers by enabling or disabling the installed services.

For example, to dedicate a computer to running and distributing reports, you can disable the presentation service on a report server computer. To dedicate a computer in a distributed installation to processing Metric Studio application requests, disable the Data Integration Service on the computer.

Note: The default values for dispatcher service and presentation service are false on computers that have the Content Manager only installed. On all other types of installations, the default values are true.

If you installed all components on several computers, you can disable appropriate services on each computer to get the distributed configuration you require. Requests are sent only to dispatchers where a given service is enabled.

Disabling a service prevents the service from loading into memory. When disabled, services do not start and therefore do not consume resources. The service does not run until you enable it.

If you disable the dispatcher service, all services that run under that dispatcher are also disabled. Only dispatcher services that are enabled can process requests.

Steps

1. Start Cognos Configuration.
2. In the **Explorer** window, under **Environment**, click **Cognos 8 service**.
3. In the **Properties** window, click the **Value** next to the service that you want to disable or enable.

   By default, all services are enabled.
4. Click the appropriate state for the services:
   - To disable the service, click **False**.
   - To enable the service, click **True**.
5. From the **File** menu, click **Save**.

Specify Resources for the Cognos 8 Service

To improve performance in a distributed environment, you can change the amount of resources that the Cognos 8 service uses by choosing a configuration template.

By default, the Cognos 8 service is configured to use minimal memory resources to optimize startup time.

The configuration template settings apply only to Tomcat, the application server that Cognos 8 uses by default. If you want to configure Cognos 8 to run on another application server, do not use Cognos Configuration to configure the resources. Instead, configure the resources within that application server environment. For more information, see "Configuring Cognos 8 for a Third-Party Application Server" (p. 293).

The Cognos 8 service is available only on the computers where you installed Content Manager or the Application Tier Components.

Steps

1. Start Cognos Configuration.
2. In the **Explorer** window, under **Environment**, **Cognos 8 service**, right-click **Cognos 8**, and click **Delete**.

   This deletes the default configuration template for the service.
3. Right-click **Cognos 8 service**, and click **New resource**, **Configuration**.

4. Type a name for the service.

   In Windows, the name you choose is used to register the service. You will see this name in the list of services running on your computer.

5. In the **Type** box, click the configuration template to use:

   - If you previously changed the default setting and now want to reduce the startup time, memory footprint, and resources used, click **Small configuration**.
   - If you want a balance between fast startup time and quick operating speeds, click **Medium configuration**.
   - If you want to maximize operating speeds and if performance is more important than fast startup time, and if your computer has a lot of resources, click **Large configuration**.

6. In the **Properties** window, edit the properties so that they are appropriate for your environment.

7. From the **File** menu, click **Save**.

Configuring Fonts

Cognos 8 components use fonts to render PDF reports on the Cognos server. Cognos 8 components also use fonts to render charts used in PDF and HTML reports.

To show output correctly, fonts must be available where the report or chart is rendered. In the case of charts and PDF reports, the fonts must be installed on the Cognos server. If a requested font is not available, Cognos 8 components substitute a different font.

Because HTML reports are rendered on a browser, the required fonts must be installed on the computer of each Cognos user who will read the HTML report. If a requested font is not available, the browser substitutes a different font.

If you want to use a new font in your reports, you must

- ❑ add the font to the list of supported fonts
- ❑ specify the file location of the new font
- ❑ map the new font to the physical font name, if required

Add Fonts to the Cognos Environment

You can add fonts to the list of supported fonts in your Cognos environment if you want to generate reports that use fonts that are currently not available. You can also remove fonts.

By default, Cognos 8 components use a set of global fonts, which are available on all Cognos server computers.

Steps

1. On each Content Manager computer, start Cognos Configuration.

2. From the **Actions** menu, click **Edit Global Configuration**.

3. Click the **Fonts** tab.
4. Click **Add**.

   Tip: To remove a font from the list of supported fonts, click the box next to the font name and then click **Remove**.
5. In the **Supported Font Name** box, type the font name and then click **OK**.
6. From the **File** menu, click **Save**.

   All global fonts, including new fonts that you add, must be installed on all Cognos computers in your environment.

If a global font is not installed on all Cognos computers, you must map the global font to an installed, physical font.

Specify the Location of Available Fonts

You must specify the installation location of all fonts, including fonts that you add to the list of supported fonts.

By default, the list of fonts consists of fonts installed in the *c8_location*\bin\fonts directory of the Cognos computer. If Cognos 8 components are installed on a Windows computer, they also use the fonts installed in the Windows font directory.

You specify the font location on all computers where Application Tier Components are installed.

Steps

1. On each Application Tier Components computer, start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, for the **Physical fonts locations** property, specify the location of the fonts.

   If there are multiple font paths, separate each path by a semicolon (;).

   If you are using an application server other than Tomcat, type the fully qualified path to the font location. For example: ***c8_location*/bin/fonts**.
4. From the **File** menu, click **Save**.

Map Supported Fonts to Installed Fonts

You can substitute global fonts, which are not installed on the computer, for physical fonts.

You map fonts on each computer where the report server is installed.

For example, you add a font to the list of supported fonts that is not installed on the Cognos computer. You can specify which font to use as a substitute.

If you want to print reports faster by using the built-in PDF fonts, you can map a global font such as Arial to one of the built-in PDF fonts, such as Helvetica-PDF, by following the steps below. You can also select one of the built-in PDF fonts for a text object in Report Studio or Query Studio. For

more information, see the Query Studio *User Guide* or the Report Studio Professional Authoring *User Guide*.

No mapping is required if you add a font to the supported font list that is installed on Cognos computers. However, you must specify the location of the font.

Steps

1. On each Application Tier Components computer, start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, click the **Value** box next to the **Physical fonts map** property, and then click the edit button.

   The **Value - Physical fonts map** dialog box appears.
4. Click **Add**.

   Tip: To remove a font, select the check box next to the font and click **Remove**.
5. In the **Global Font Name** box, type the name of the font you added to the supported font list.
6. Click the **Physical Font Name** box.
7. If you know the physical font name, type it. Otherwise, click the edit button. In the **Physical Font Name** dialog box, click **Search Now** and then click a font name from the results.
8. Repeat steps 4 to 7 for each global font that requires mapping.
9. Click **OK**.
10. From the **File** menu, click **Save**.

Now, if required, you must specify the installation location of the fonts.

Change the Default Font for PDF Reports

You can change the default font that Cognos 8 components use for PDF reports. You see this default font when you open a report.

You change the default font on the computer where Content Manager is installed. After you make the change, the font becomes the default for all computers in your installation. You change the font used for PDF reports using Cognos Configuration.

Ensure that the default font is installed on all computers in your Cognos installation.

Steps

1. On each Content Manager computer, start Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **General** tab.
4. In the **Value** box, for **Default font**, type the font you want to use as the default for reports.

5. Click **OK**.
6. From the **File** menu, click **Save**.
7. On all Application Tier Components computers, ensure that the installation location of the default font is specified in the **Physical fonts locations** property (under **Environment** in the **Explorer** window) or that the font is in the Windows font directory.

Configure Embedded Fonts for PDF Reports

When a PDF report opens in Adobe Reader, all the fonts used in that report must be available. Fonts must be either embedded in the report or installed on the user's computer. If a font is not available in either of these locations, Adobe Reader tries to substitute an appropriate font. This substitution may cause changes in the presentation of the report or some characters may not be displayed.

To ensure that PDF reports appear correctly in Adobe Reader, Cognos 8 embeds required fonts in reports by default. To minimize the file size, Cognos 8 embeds only the characters (also called glyphs) used in the report rather than all characters in the font set. Cognos 8 embeds fonts only if they are licensed for embedding. The license information is stored in the font itself and is read by Cognos 8.

If you are confident that the fonts used in reports are available on users' computers, you can limit or eliminate embedded fonts to reduce the size of PDF reports. When limiting fonts, you specify whether a font is always or never embedded, using an embedded fonts list in Cognos Configuration.

Steps

1. On the Content Manager computer, start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, under **Font Settings**, click the value for **Fonts to embed (Batch report service)** or **Fonts to embed (Report service)**, and then click the edit button.
4. If you are not using the default fonts directory or if you want to add a path to an additional directory, in the **Fonts to Embed in PDF Reports** dialog box, specify the new path in the font paths box.

   Tip: Click **Search Now** to get a list of the available fonts in the specified path or paths.
5. For a font that will always be available on users' computers, scroll to the font name, and click the **Never** check box.

   Cognos 8 does not embed the font with any reports. Adobe Reader picks up the font from the user's computer when the report is opened.
6. For a font that may not always be available on the users' computers, scroll to the font name and click the **Always** check box.

   Cognos 8 embeds the font with all reports that use it. Adobe Reader uses the embedded font when the report is opened.

7. Click **OK**.

Saved Report Output

By default, report output files are saved in the content store. You have the option of saving a copy of the report output in another file location that is outside or inside Cognos 8. If you use this option, a descriptor file with an _descr extension is also saved. Saved files are not managed by Cognos 8.

Save Report Output Outside Cognos 8

If you configure a file system location that is outside of Cognos 8, you can then share the report output with external applications or people who don't have Cognos 8. This is how most report output files are saved.

To use this feature, you must first configure a root directory in Cognos Configuration. An administrator must then set the file location in Cognos Administration. For more information, see the topic about setting a file location for report output saved outside of Cognos 8, in the *Administration and Security Guide*.

Steps

1. Create a directory for your file system.

   Tip: Ensure that the directory is accessible to users and separate from the installation directory. For example, in a distributed installation, an archive folder such as *servername**directory* could be used.

2. On the Content Manager computer, start Cognos Configuration.

3. From the **Actions** menu, click **Edit Global Configuration**.

4. In the **Global Configuration** window, click the **General** tab.

5. For **Archive Location File System Root**, type a URI using the format

   file://*directory*

   where *directory* is the directory that you created in step 1.

   The file:// portion of the URI is required. Windows UNC names, such as *servername**directory*, can be used. If so, the URI must be formatted as follows:

   file://*servernamedirectory***

6. To confirm that the correct location will be used, click **Test**.

7. Click **OK**.

8. From the **File** menu, click **Save**.

The administrator must now configure the file location. For information, see the topic about setting a file location for report output saved outside of Cognos 8, in the *Administration and Security Guide*.

Save Report Output Inside Cognos 8

If you configure a file system location that is inside Cognos 8, you can then use the report output again. This may also be useful for archive purposes, because files that are saved in the Content Store may be deleted regularly due to retention rules.

To use this feature, you must first enable the **Save report outputs to a file system** property in Cognos Configuration. An administrator must then configure the file location using the CM.OutPutLocation parameter in Cognos Administration. For more information, see the topic about setting a file location for report output saved inside Cognos 8, in the *Administration and Security Guide*.

Steps

1. Create a directory for your file system.

   Tip: Ensure that the directory is accessible to authorized users only.

2. On the Content Manager computer, start Cognos Configuration.
3. In the **Explorer** window, click **Data Access**, **Content Manager**.
4. For the **Save report outputs to a file system** property, click **True**.
5. To test the connection to the report output directory, from the **Actions** menu, click **Test**.
6. From the **File** menu, click **Save**.

The administrator must now configure the file location using the CM.OutPutLocation parameter. For information, see the topic about setting a file location for report output saved inside Cognos 8, in the *Administration and Security Guide*.

Change the Location of Map Charts for Report Studio

Cognos 8 comes with a set of sample map charts that you can use in Report Studio. By default, the map charts are stored in the *c8_location*\maps directory on the Application Tier Components computer. You can change the location of the map charts by using Cognos Configuration.

For more information about using map charts, see the Report Studio *User Guide*.

For information about using custom maps from third-party sources, see the Map Manager *Installation and User Guide*.

Steps

1. On the Application Tier Components computer, start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, click the value for **Map files location**.
4. Click the edit button.
5. In the **Select Folder** window, navigate to the directory you want and then click **Select**.
6. From the **File** menu, click **Save**.

Configuring the SSL Protocol

The Secure Sockets Layer (SSL) protocol is used to secure communication between Cognos components installed on the same computer or on different computers.

In addition, you may want to set up SSL connections between Cognos components and other servers. You must ensure that SSL is set up for the other servers and then you must set up a shared trust between Cognos components and the other servers.

After configuring the SSL protocol, you can select and rank cipher suites, which control the quality of protection used in the SSL connection.

To configure SSL protocol, do the following:

- ❑ Configure SSL for Cognos components (p. 211).
- ❑ Set up shared trust between Cognos components and other servers, if required (p. 213).
- ❑ Select and rank Cipher Suites to be used in an SSL connection, if required (p. 214).

Configure SSL for Cognos 8

You can configure Cognos components to use the SSL protocol for

- internal connections only
- external connections only
- internal and external connections
- connections to local and remote log servers

If you configure SSL only for internal connections, Cognos components on the local computer communicate using this protocol. The dispatcher listens for secure connections on a different port than for remote, http requests. Therefore, you must configure two dispatcher URIs.

If you configure SSL only for external connections, communications from remote Cognos components to the local computer use the SSL protocol. You must configure the dispatcher to listen for secure, remote requests on a different port than local, HTTP requests. You must also configure the Content Manager URIs and the dispatcher URI for external applications to use the same protocol and port as the external dispatcher.

If you configure SSL for all connections, the dispatcher can use the same port for internal and external connections. Similarly, if you do not use SSL for local or remote communication, the dispatcher can use the same port for all communications.

You must also update the Content Manager URIs, Dispatcher URI for external applications, and Gateway URI to use SSL, if required.

Tomcat Connectors

If the internal dispatcher URI is prefixed with http but the external dispatcher URI is prefixed with https, or vice versa, both the non-SSL Coyote HTTP/1.1 and SSL Coyote HTTP/1.1 connectors are enabled in the server.xml file.

If the internal and external dispatcher URIs use different protocol or ports, the internal dispatcher port is accessible only to the components on the local computer. The internal dispatcher URI must also specify localhost.

Single Computer Installations

In single computer installations, if you are running Cognos 8 without SSL, you must stop the service before adding SSL to your configuration. After you save the configuration with SSL settings, you can restart the service.

Distributed Installations

In distributed installations, if you are using the Cognos certificate authority service, you must first configure all Cognos computers to use the non-secure (http) protocol before you configure Cognos components to use the SSL protocol. You must do this because you cannot set up the SSL protocol before trust has been established.

Also, ensure that you follow the required order of configuring computers in a distributed environment. That means that you must first configure the computer where the default active Content Manager is installed and then start the services on this computer before you configure other computers or start services on other computers. By first configuring the default active Content Manager computer and starting the services, you ensure that the certificate authority service on the default active Content Manager computer can issue certificates to other computers in the Cognos environment.

After you configure all computers in the distributed installation to use the default, non-secure protocol, we recommend that you test your installation to ensure that Cognos components are working properly. After you test your installation, you can configure the SSL protocol.

When you configure Cognos 8 to use the SSL protocol, ensure that you first configure the default active Content Manager computer to use the protocol and start the services on the default active Content Manager computer. After you do this, you can configure the SSL protocol on other Cognos computers in your environment.

Add a Computer to an Installation

If you add a computer to an SSL-enabled environment, you will be prompted to temporarily accept trust for a certificate when you save the configuration. Accepting the temporary certificate will allow permanent trust to be established with the Content Manager computer.

Add a Component to a Computer

You can later add a component to the same location as other Cognos components. If you add the component to a different location on the same computer as other Cognos components, you will be prompted to temporarily accept trust for a certificate when you save the configuration. Accepting the temporary certificate will allow permanent trust to be established between the new component and the Content Manager computer.

Steps

1. Start Cognos Configuration.

2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, type the appropriate values for the **Internal dispatcher URI** and **External dispatcher URI** values:
   - To configure SSL for internal connections only, for the **Internal dispatcher URI** property, type **https** and a port for SSL communication. For the **External dispatcher URI** property, type **http** and use the default or another available port.

     If you use Tomcat, the **Internal dispatcher URI** property must also specify **localhost**.

     The ports in the two dispatcher URIs must be different.
   - To configure SSL for external connections only, for the **External dispatcher URI** property, type **https** and a secure port. For the **Internal dispatcher URI** property, type **http** and use the default or another available port.

     If you use Tomcat, the **Internal dispatcher URI** property must also specify **localhost**.

     The ports in the two dispatcher URIs must be different.
   - To configure SSL for all connections, type the same URI for both the **Internal dispatcher URI** and **External dispatcher URI** properties. Type **https** and a secure port, such as 9343.

   Note: You do not have to use port 9343, the default SSL port. You can choose any available port.
4. Configure the SSL protocol for the other environment URIs, including the **Content Manager URIs**, the **Dispatcher URI for external applications**, and **Gateway URI**.
   - For internal connections only, type **https** in the URIs that contain localhost.
   - For external connections only, type **https** in the URIs that do not contain localhost.
   - For all connections, type **https** in all the URIs.
5. In the **Explorer** window, click **Security**, **Cryptography**.
6. To use SSL protocol, you must specify passwords for the Cognos 8 encryption key stores. There are more settings under **Security**, **Cryptography**, **Cognos**.
7. From the **File** menu, click **Save**.

Set Up Shared Trust Between Cognos Servers and Other Servers

If you want to use the default Cognos certificate authority and you want to use SSL for connections from other servers to Cognos servers, you must add the Cognos certificate to the trust store on the other servers.

Note: If you use browsers to connect to Cognos components, the browsers automatically prompt users to update their trust stores.

If you want the connection between Cognos servers and the other server to be mutually authenticated, you must also copy the certificate from your certificate authority to the trust store for Cognos servers.

If you have configured Cognos components to use a third-party certificate authority (CA), you do not have to set up shared trust between Cognos server and other servers.

Steps to Copy the Cognos Certificate to Another Server

1. Go to the *c8_location*\bin directory.
2. Extract the Cognos certificate by typing the following command:
   - On UNIX or Linux, type

     ThirdPartyCertificateTool.sh -E -T -r ***destination_file*** **-k** ***c8_location*****/configuration/signkeypair/jCAKeystore -p** ***password***
   - On Windows, type

     ThirdPartyCertificateTool.bat -E -T -r ***destination_file*** **-k** ***c8_location*****\configuration\signkeypair\jCAKeystore -p** ***password***
3. Import the certificate to the trust store on your server.

   For information on updating the server trust store, see the documentation for your server.

Steps to Copy the CA Certificate to Cognos Servers

1. Copy the certificate from your certificate authority to a secure location on the Cognos server.

   Ensure that the CA certificate is in Base-64 encoded X.509 format.
2. Import the CA certificate by typing the following command:
   - On UNIX or Linux, type

     ThirdPartyCertificateTool.sh -T -i -r ***CA_certificate_file*** **-k** ***c8_location*****/configuration/signkeypair/jCAKeystore -p** ***password***
   - On Windows, type

     ThirdPartyCertificateTool.bat -T -i -r ***CA_certificate_file*** **-k** ***c8_location*****\configuration\signkeypair\jCAKeystore -p** ***password***

Select and Rank Cipher Suites for SSL

An SSL connection begins with a negotiation in which the client and server present a list of supported cipher suites in a priority sequence. A cipher suite provides the quality of protection for the connection. It contains cryptographic, authentication, hash, and key exchange algorithms. The SSL protocol selects the highest priority suite that the client and the server both support.

Cognos provides a list of supported cipher suites for SSL. You can eliminate cipher suites that do not meet your requirements and then assign a priority, or preference, to the remaining cipher suites. The selected cipher suites are presented in priority sequence for the client and server sides of the negotiation. At least one of the selected cipher suites between the client and server platforms must match.

The list of supported cipher suites is dynamically generated on each computer, and depends on the Java Runtime Environment (JRE) or whether you have third-party cryptographic software installed on the computer. If you have made changes to a computer, such as upgraded the JRE or installed software that has upgraded the JRE, this may affect the supported cipher suites available on that computer. If you no longer have a supported cipher suite that matches the other computers in your environment, you may have to change the JRE on the computer to match the other computers in your environment.

Steps

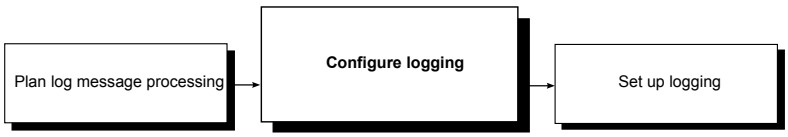
1. Start Cognos Configuration.
2. In the **Explorer** window, click **Cryptography**, **Cognos**.
3. In the **Properties** window, click the **Value** column for the **Supported ciphersuites** property.
4. Click the edit button.
   - To move a cipher suite to the **Current values** list, click the check box in the **Available values** list and then click **Add**.
   - To move a cipher suite up or down in the **Current values** list, click the check box and then click the up or down arrows.
   - To remove a cipher suite from the **Current values** list, click the check box and then click **Remove**.
5. Click **OK**.
6. From the **File** menu, click **Save**.

Configuring Log Messages

Log messages are an important diagnostic tool for investigating the behavior of Cognos 8. In addition to error messages, log messages provide information about the status of components and a high-level view of important events. For example, log messages can provide information about attempts to start and stop services, completion of processing requests, and indicators for fatal errors. Audit logs, which are available from a logging database, provide information about user and report activity.

The Cognos 8 services on each computer send information about errors and events to a local log server. A local log server is installed in the *c8_location*/logs folder on every Cognos 8 computer that contains Content Manager or Application Tier Components. Because the log server uses a different port from the other Cognos 8 components, it continues to process events even if other services on the local computer, such as the dispatcher, are disabled.

The following workflow shows the tasks that are required to prepare for logging.



- During planning, determine the logging configuration that is suitable for your environment. For example, evaluate various log message destinations, such as remote log servers and log files, such as the UNIX or Linux syslog or the Windows NT Event log, in addition to the local log file. You can also send only audit logging information to a third-party database. Consider security, such as methods available for protecting log files from system failures and user tampering. For information about planning, see the *Architecture and Deployment Guide*.
- During configuration, define the startup properties for logging, such as connection settings for third-party databases. You must also create a logging database if you plan to collect audit logs. If communication between a local log server and a remote log server must be secured, make the appropriate configuration changes on both Cognos 8 computers. For information about configuring logging, see the *Installation and Configuration Guide*.
- When setting up logging, specify the level of detail to log to focus messages on the information that is relevant in your organization. Audit reports may also be set up to track user and report activity. For information about setting up logging, see the *Administration and Security Guide*.

For information about using log messages to solve problems and resolving logging-related issues, see the Troubleshooting section of the *Administration and Security Guide*.

Log Message Destinations

A local log server is automatically installed when you install Content Manager or the Application Tier Components. You can specify one or more destinations where the local log server sends log messages:

- a remote log server
- a file
- a database
- the UNIX or Linux syslog or the Windows NT Event log

For information about log messages, see the *Architecture and Deployment Guide*.

To configure log messages:

- Create the logging database, if sending messages to a database, using the same procedure as to create the content store database (p. 118).

  Important: For DB2, you must create an additional regular user tablespace with a page size of 8k for Cognos 8 components to create the logging database.
- Set up the database client, if required.
- Specify the log messages destination.

A Remote Log Server

In a distributed installation, you can configure the log server on each Cognos 8 computer to send log messages to a single remote log server, which acts as a common log server. You can then configure the common log server to send the log messages to a local file or database on the same or another computer.

If the remote log server becomes unavailable, log messages are redirected to recovery files on the local computer in the *c8_location*\logs\recovery\remote directory. These recovery files have timestamp information in their file names, and are not readable like regular log files. When the remote log server becomes available, an automatic recovery process moves all log information to the remote log server and deletes the local log files.

A File

The log server is configured by default to send log messages to the *c8_location*/logs/cogserver.log file. If the default log file does not exist when the Cognos 8 service starts, it is created automatically.

You can configure the log server to send log messages to a different file. If you configure a different log file, Cognos 8 attempts to automatically create this file on startup, in addition to the default log file. If the location for the configured log file is different from the *c8_location*/logs directory, you must ensure the path to the log file exists before starting the Cognos 8 service. For example, if you configure the log server to send messages to the c:/log_files/cognos.log file, Cognos 8 attempts to automatically create the cognos.log file in the c:/log_files folder. If this folder does not exist, Cognos 8 does not create the cognos.log file and no log messages can be recorded in it. Note that these log messages are not recorded in the default log file. Although Cognos 8 automatically creates the default log file even when another log file is configured, the default log file is not used as a backup.

A Database

The log server can also send audit logs to a database on the same or another computer. Audit logs provide information about user and report activity.

The logging database has the same configuration and user account requirements as the content store database. After you configure Cognos 8 components to send messages to a logging database, and restart the Cognos 8 service, Cognos 8 components create the required tables and table fields. You can test the connection to the logging database before you restart the Cognos 8 service.

Set Up the Database Client for a Logging Database

After you create a database for audit logs, additional steps are required to set up the database client if you use Oracle, DB2, or Sybase as the database server. If you use a Microsoft SQL Server database, the JSQLConnect.jar file is installed to the appropriate location by default. The only additional step is to ensure that the Microsoft SQL Server uses TCP/IP connectivity.

Note: You cannot use Cognos Content Database as a logging database.

If you use an Oracle or Sybase database, you must set up the JDBC driver on all Application Tier Components computers with a connection to the logging database. You must also set up the JDBC

driver on the Content Manager computer, unless you are using the same type of database for the log messages as you use for the content store.

If you use a DB2 database, you must set up the database client software and the JDBC 2.0 driver on all Application Tier Components computers with a connection to the logging database. You must also set up the database client software and the JDBC 2.0 driver on the Content Manager computer, unless you are using the same type of database for the log messages as you use for the content store.

Note: In a distributed environment, the local log server on an Application Tier Component computer may send log messages to a remote log server, which then sends messages to the logging database. For Oracle, Sybase, and DB2, the appropriate JDBC driver and database client software (DB2 only) is required only on the Application Tier Components computer with the remote log server that connects to the logging database.

Steps for Oracle

1. On the computer where Oracle is installed, go to the ORACLE_HOME/jdbc/lib directory.
2. Copy the ojdbc14.jar file to the *c8_location*/webapps/p2pd/WEB-INF/lib directory on the appropriate Content Manager or Application Tier Components computers.

   If the directory contains the classes12.jar file, delete it before installing the ojdbc14.jar file.

Steps for DB2

1. Install the DB2 client software on the appropriate Content Manager or Application Tier Components computers.
2. If the logging database is on a different computer from the log server, configure a database alias to the logging database:
   - On Windows, run the DB2 Client Configuration Assistant.
   - On UNIX or Linux, use the DB2 command line interface.

   Note: If the logging database and log server are on the same computer, the logging database name is automatically used to create an alias.
3. On Windows, stop the DB2 services and the HTML Search Server.
4. To copy the JDBC2 driver, copy the *DB2_installation*/sqllib/java/db2java.zip file to the *c8_location*/webapps/p2pd/WEB-INF/lib directory.
5. Rename the db2java.zip file to db2java.jar.
6. On Windows, restart the DB2 services and the HTML Search Server.
7. Repeat this entire procedure on the appropriate Content Manager or Application Tier Components computers.

Steps for Sybase

1. On the computer where Sybase is installed, enable the JDBC driver using the following script:

Sybase_location/jConnect-5_5/sp/sql_server12.5.sql

2. Go to the *Sybase_location*/jConnect-5_5/classes directory.
3. Copy the jconn2.jar file to the *c8_location*/webapps/p2pd/WEB-INF/lib directory on the appropriate Content Manager or Application Tier Components computers.

Specify the Log Messages Destination

You can configure a type of destination for the log messages, and then configure properties for the specific destination. You can also configure more than one destination for log messages.

Steps

1. If the destination is a database, ensure that you
   - created the logging database (p. 118)
   - set up the database client (p. 217)
2. On the computer where you installed Content Manager or the Application Tier Components, start Cognos Configuration.
3. In the **Explorer** window, under **Environment**, click **Logging**.
4. In the **Properties** window, set the log server properties.
   - If you want to use TCP between Cognos 8 components on a computer and its local log server, set the **Enable TCP** property to **True**.

     The default setting, UDP, provides faster communication with a lower risk of lost connections than TCP. However, the risk of losing a local TCP connection is low. TCP is always used for communication between a local log server and a remote log server.
   - If you want to change the number of threads available to the local log server, type the value in the **Local log server worker threads** property.

     You can set a value between 1 and 20. The default value of 10 is recommended. However, if you have a high number of log messages, you may want to allocate more threads to improve performance.
   - If you want UTF-8 encoding applied to log messages written to a file, set the **Use UTF8** property to **True**.

     If the Cognos 8 component is using multibyte encoding, you must set this property to True and use a UTF-8 editor to view the log file. Otherwise, the log file may contain unreadable characters.
5. In the **Explorer** window, under **Environment**, right-click **Logging**, and click **New resource**, **Destination**.
6. In the **Name** box, type the name of the destination.
7. In the **Type** list, click the type of destination and then click **OK**.

8. If the destination is a file, in the **Properties** window, type the appropriate values for the mandatory and optional properties.
9. If the destination is a remote log server, in the **Properties** window, type the appropriate values for the mandatory and optional properties.

   If the **Internal dispatcher URI** of the destination Cognos 8 computer is configured to use SSL (p. 211), in the **Properties** window, set the **Enable SSL** property to **True**.

   You must later specify the log messages destination when you configure the remote log server.
10. If the destination is a database, in the **Explorer** window, under **Logging**, specify the type of database and its properties, as follows:
    - Right-click the database name, and click **New resource**, **Database**.
    - In the **Name** box, type the name of the destination.
    - In the **Type** list, click the type of database and then click **OK**.
    - In the **Properties** window, type the appropriate values for the mandatory and optional properties.

      For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property.

      To connect to a named instance, you must specify the instance name as a JDBC URL property or a data source property. For example, you can type **localhost\instance1**. If no instance name property is specified, a connection to the default instance is created.

      Note that the properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

      jdbc:JSQLConnect://localhost\\instance1/user=sa/*more properties as required*
    - Test the connection to the new database. In the **Explorer** window, under **Environment**, right-click **Logging** and click **Test**.

      Cognos 8 components connect to the database. If you configured more than one database for logging messages, Cognos 8 components test all of the databases.
11. Repeat steps 5 to 10 for each destination to which you want the log server to send messages.
12. From the **File** menu, click **Save**.
13. In the **Explorer** window, click **Cognos 8 service**, **Cognos 8**.
14. From the **File** menu, click **Restart**.

    If you selected a database as the destination, Cognos 8 components create the required tables and fields in the database that you created.

If the destination was a remote log server, configure and start the remote log server. Then restart the Cognos 8 service on the local computer.

If the destination was a database, you can use Cognos 8 components to run log reports from the database.

You can also set the logging level, which controls the amount of detail and type of messages that are sent to a log file or database. For instructions, see the *Administration and Security Guide*.

Changing Global Settings

You change global settings

- to customize language support for the user interface
- to customize currency support
- to customize content locale support
- to map the language used in the product user interface
- to map content locales
- to add fonts to your Cognos environment
- to customize the default time zone
- to change the encoding for email messages
- to customize cookie settings

By default, Cognos 8 components ensure that all locales, which may come from different sources and in various formats, use a normalized form. That means that all expanded locales conform to a language and regional code setting.

Each computer has a default system locale and one user locale per user. The user locales may be different from the default system locale.

Important: If you change global settings on one Content Manager computer, you must make the same changes on the other Content Manager computers.

Customize Language Support to the User Interface

Use the Product Locales table to add or remove the user interface language support. For example, if you do not require a German user interface, you can remove the language from the list.

If you change the user interface language of the product, data is not affected.

Before you can add language support to the user interface, you must install the language files on all computers in your distributed installation. For more information, contact your Cognos support representative.

Adding languages to the Cognos environment does not guarantee that your computer has a font that can display Web pages in your preferred languages. Ensure that you install the appropriate

language packs to support the character sets you use. For information about installing language packs, see the Cognos Supplementary Languages *Installation and Configuration Guide*.

Steps

1. On each Content Manager computer, start Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Product Locales** tab.
4. Click **Add**.

   Tip: To remove support, select the check box next to the **Supported Locale** and then click **Remove**.
5. In the second column, type the language portion of a locale.
6. Repeat steps 3 to 5 for other language support that you want to add.
7. Click **OK**.
8. From the **File** menu, click **Save**.

Customizing Currency Support

If you require additional currencies or want to remove some from the user interface, you can update the list of supported currencies in the Currencies table. If you use Japanese or Korean currencies, you must configure support so that Japanese Yan and Korean Won characters display correctly.

Add Currencies to Cognos 8

You can add supported or unsupported currencies to the user interface. You add supported currencies in Cognos Configuration. You add unsupported currencies to the i18n_res.xml file that is provided in Cognos 8.

By default Cognos 8 components show only a subset of supported currencies in the user interface. Currencies are identified by their ISO 4217 currency code. The complete list of supported currencies that can be added are listed in the i18n_res.xml file in the *c8_location*\bin directory.

If you add a currency code that is not supported by Cognos, you must manually add it to the i18n_res.xml file in the *c8_location*\bin directory. Copy this file to each Cognos computer in your installation.

Adding currencies to the Cognos environment does not guarantee that your computer has a font with the required characters to display the currency. Ensure that you install the appropriate language packs to the support currency symbols you use. For example, to display the Indian currency symbol (rupee) correctly, you must run a Japanese operating system or install a Japanese language. For

information about installing language packs, see the Cognos Supplementary Languages *Installation and Configuration Guide*.

Steps

1. On each Content Manager computer, start Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Currencies** tab.
4. Click **Add**.

   Tip: To remove support, select the check box next to the supported item and then click **Remove**.
5. In the second column, type an appropriate value.

   The value you add must comply with ISO 4217 codes for the representation of currencies and formats. Usually the value you add is a three-letter alphabetic code. The first two characters are letters representing the ISO 3166 country code for the country the currency is from. The additional letter represents the first letter of the currency.
6. Repeat steps 3 to 5 for other types of support that you want to add.
7. From the **File** menu, click **Save**.

Configure Support for Japanese Yen and Korean Won Characters

The Japanese Yen and Korean Won characters are stored as U+00A5 and U+20A9, respectively, in the Unicode standard character map. However, the usage of these values is not universal and U+005C is often used for the Yen character in Japan and the Won character in Korea. Depending on the fonts you have available, the character stored as U+005C can appear as a backslash rather than a Yen or Won character. For example, if the server does not have the appropriate language font and uses the standard fallback font provided by Cognos, Andale WT, the U+005C value is used as a backslash.

Cognos also provides an Andale WT Japanese and Andale WT Korean font. These fonts map the U+005C value as a Yen or Won character. The Andale WT Japanese and Andale WT Korean fonts are available on the Cognos 8 Supplementary Languages CD. To use these fonts, you must install them from the Cognos 8 Supplementary Languages CD and then modify the GlobalReportStyles.css file.

Steps to Install the Fonts for Yen and Won Characters

1. Use the installation wizard on the Supplementary Languages CD on each computer that contains Application Tier components.

   For more information, see the Cognos 8 Supplementary Languages *Installation and Configuration Guide*.
2. On the Component Selection page of the installation wizard, expand the **Additional Language Fonts** option, and select the font you want to install.
3. Follow the instructions in the installation wizard to complete the installation.

The fonts are copied to the *c8_location*\bin\fonts directory. This font location is defined in the **Physical fonts location** value in Cognos Configuration under **Local Configuration**, **Environment**. If you move the fonts to another location, ensure that the new location is added to the **Physical fonts location** value.

Steps to Update the Style Sheet

1. Open the GlobalReportStyles.css style sheet in a text editor.

   The GlobalReportStyles.css style sheet is located in the *c8_location*\bin directory.

2. Enable one of the following sections and modify it as shown below:

   - ```
     /* For Japanese: */

     .pg,

     .pp

     {

     font-family: 'MS UI Gothic', 'Andale WT J' , Tahoma, arial, geneva,
     helvetica, sans-serif;

     }
     ```

   - ```
     /* For Korean: */

     .pg,

     .pp

     {

     font-family: Gulim, 'Andale WT K' , Tahoma, arial, geneva, helvetica,
     sans-serif;

     }
     ```

   The PDF generator uses the first available font on the server and includes all the characters in the string to be displayed. If you prefer to use other fonts on your server, you can insert them into the list.

3. Save the GlobalReportStyles.css file.

4. Restart the Cognos 8 server.

Any changes that you make to the style sheet are overwritten if you upgrade Cognos 8. You must repeat this procedure following an upgrade.

Customize Content Locale Support

To ensure users see reports, data or metadata in their preferred language, or specific to their region, you can add partial locales (language) or complete locales (language-region) to the Content Locales table. This way, if content is available in different languages, or in different locales, it is rendered to users based on their user locale. By default, content locale overrides product locale in the portal for some content.

If you view reports in Thai language, digits are not supported.

If a locale is not required, you can remove it from the list. You must leave at least one content locale in the list for the report server to operate.

Adding incomplete locales (languages) to the Cognos environment does not guarantee that your computer has a font that can display Web pages in your preferred languages. Ensure that you install the appropriate language packs to support the character sets you use. For information about installing language packs, see the Cognos Supplementary Languages *Installation and Configuration Guide*.

Steps

1. On each Content Manager computer, start Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Content Locales** tab.
4. Click **Add**.

   Tip: To remove support, select the check box next to the supported item and then click **Remove**.
5. In the second column, type an appropriate value.
   - To add language support for report data and metadata, type a partial local (language) setting.
   - To add support specific to a region, type a complete locale (language-region) setting.
6. Repeat steps 3 to 5 for each additional locale that you want to support.
7. From the **File** menu, click **Save**.

Map Content Locales

Use the Content Locale Mappings table to map user locales to a complete (language-region) or partial (language) locale. You can also map a user's preferred language to another language if content is not available in the user's preferred language.

For example, if a report or scorecard is not available in a preferred language, for example Vietnamese, but is available in French and German, you can use the Content Mappings table to map the preferred language (Vietnamese) to another language (French or German). This way, you see the report or scorecard in the mapped language.

By default, the Content Locale Mappings table includes locales that do not contain the region. This allows you to use only the language portion of the locale when you specify locale settings and ensures that you always see the correct information. For example, in a multilingual database, data is usually available in different languages, such as French (fr), Spanish (es) and English (en), rather than being available in different locales, such as English Canada (en-ca), English United States (en-us), or French France (fr-fr).

The following examples show the method that Cognos 8 components use to determine which report or scorecard the user sees if the multiple language versions are available.

Example 1

A report is available in Content Manager in two locales, such as en-us (English-United States) and fr-fr (French-France), but the user locale is set to fr-ca (French-Canadian). Cognos 8 uses the locale mapping to determine which report the user sees.

First, Cognos 8 checks to see if the report is available in Content Manager in the user's locale. If it is not available in the user's locale, Cognos 8 maps the user's locale to a normalized locale configured on the Content Locale Mapping tab. Because the user's locale is fr-ca, it is mapped to fr. Cognos 8 uses the mapped value to see if the report is available in fr. In this case, the report is available in en-us and fr-fr, not fr.

Next, Cognos 8 maps each of the available reports to a normalized locale. Therefore, en-us becomes en and fr-fr becomes fr.

Because both report and the user locale maps to fr, the user having the user locale fr-ca will see the report saved with the locale fr-fr.

Example 2

The user's locale and the report locales all map to the same language. Cognos 8 chooses which locale to use. For example, if a user's locale is en-ca (English-Canada) and the reports are available in en-us (English-United States) and en-gb (English-United Kingdom), Cognos 8 maps each locale to en. The user will see the report in the locale setting that Cognos 8 chooses.

Example 3

The report and the user locales do not map to a common language. Cognos 8 chooses the language. In this case, you may want to configure a mapping. For example, if a report is available in en-us (English-United States) and fr-fr (French-France), but the user locale is es-es (Spanish-Spain), Cognos 8 chooses the language.

Steps

1. On each Content Manager computer, start Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **Content Locale Mapping** tab.
4. Click **Add**.
5. In the **Key** box, type the user locale:
   - To ensure all regions for a user locale see content in a specific language, type the language portion of the locale, followed by a dash (-) and an asterisk (*).

     For example, type **fr-***
   - To ensure a user locale (language-region) sees content in a specific language, type the complete locale.

     For example, type **fr-ch**

- To map a preferred language to another language, type the preferred language portion of the locale.

  For example, type **zh**

Tip: To specify the locale to use for a range of keys, use the wildcard character (*) with the **Key** value and then, in the **Locale Mapping** box, type the locale. For example, if you want all the German keys to use the German locale, type **de*** in the **Key** box and type **de** in the **Locale Mapping** box.

6. In the **Locale Mapping** box, type the language portion of the locale.

   User locales specified in the **Key** box will see content in this language.

7. Repeat steps 3 to 5 for other mappings you want to do.

8. Click **OK**.

9. From the **File** menu, click **Save**.

Map Product Locales

Use the Product Locale Mappings table to specify the language used in the user interface when the language specified in the user's locale is not available.

You can ensure that all regions for a locale use the same language, or that a specific, complete locale (language-region) uses a particular language.

By default, the user sees the product interface in the language that matches the language setting of the user locale.

Steps

1. On each Content Manager computer, start Cognos Configuration.

2. From the **Actions** menu, click **Edit Global Configuration**.

3. Click the **Product Locale Mappings** tab.

4. Click **Add**.

5. In the **Key** box, type the user locale:

   - To ensure all regions for a locale see the user interface in a specific language, type the language portion of the locale, followed by a dash (-) and an asterisk (*).

     For example, type **es-***

   - To ensure a complete locale (language-region) see the user interface in a specific language, type the complete locale.

     For example, type **es-es**

   - To map a preferred language to another language, type the preferred language portion of the locale.

For example, type **zh**

Tip: To specify which locale to use as the default, use the wildcard character (*) for the **Key** value and then, in the **Locale Mapping** box type the locale.

6. In the **Locale Mapping** box, type the language portion of the locale.

   User locales specified in the **Key** box will see content in this language.

7. Repeat steps 3 to 5 for other mappings you want to do.

8. Click **OK**.

9. From the **File** menu, click **Save**.

Customize the Server Time Zone

You can customize the time zone used by Content Manager by selecting a different server time zone in Cognos Configuration.

For UNIX installations that do not support a Java-based graphical user interface, you can view the list of acceptable time zones by opening Cognos Configuration on the Windows computer where Framework Manager is installed.

Content Manager is configured to use the time zone of your operating system by default. All scheduled activities in Cognos 8 are set using this time zone. In addition, users in Cognos Connection use this time zone if they set their preferences for the default time zone. For more information about setting user preferences in Cognos Connection, see the *Administration and Security Guide*.

Steps

1. Start Cognos Configuration.

2. From the **Actions** menu, click **Edit Global Configuration**.

3. In the **Global Configuration** window, click the **General** tab.

4. Click the **Value** column for **Server time zone** and select another time zone from the list.

5. From the **File** menu, click **Save**.

Change Encoding for Email Messages

By default, Cognos 8 components use UTF-8 encoding in emails. This value sets the default encoding used by the delivery service in this instance for all email messages. You may have older email clients or send email from Cognos 8 to cell phones and PDAs that do not recognize UTF-8. If so, you can change the email encoding to a value that works on all your email clients (for example, ISO-8859-1, Shift-JIS). Each instance of Cognos 8 that has an available delivery service must be changed.

The specified encoding affects the entire message, including the subject, attachments, attachment names, and plain or HTML body text.

Character set	Supported encoding value
UTF-8	utf-8
Western European (ISO 8859-1)	iso-8859-1
Western European (ISO 8859-15)	iso-8859-15
Western European (Windows-1252)	windows-1252
Central and Eastern European(ISO 8859-2)	iso-8859-2
Central and Eastern European (Windows-1250)	windows-1250
Cyrillic (ISO 8859-5)	iso-8859-5
Cyrillic (Windows-1251)	windows-1251
Turkish (ISO 8859-9)	iso-8859-9
Turkish (Windows-1254)	windows-1254
Greek (ISO 8859-7)	iso-8859-7
Greek (Windows-1253)	windows-1253
Japanese (EUC-JP)	euc-jp
Japanese (ISO-2022-JP)	iso-2202-jp
Japanese (Shift-JIS)	shift_jis
Traditional Chinese (Big5)	big5
Simplified Chinese (GB-2312)	gb2312
Korean (EUC-KR)	euc-kr
Korean (ISO 2022-KR)	ISO 2022-KR
Korean (KSC-5601)	ksc_5601
Thai (Windows-874)	windows-874

Character set	Supported encoding value
Thai (TIS-620)	tis-620

Steps

1. Start Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. In the **Global Configuration** window, click the **General** tab.
4. Click the **Value** column for the **Email Encoding** property.
5. Scroll to the desired setting and click it.
6. From the **File** menu, click **Save**.

Customize Cookie Settings

Based on the requirements of your Cognos environment, you may need to modify the settings that Cognos 8 components use to create cookies. You can use Cognos Configuration to customize the cookie domain, path, and secure flag.

Cognos 8 components determine the cookie domain from the HTTP request submitted by the client, which is typically a Web browser. In most network configurations, HTTP requests pass through intermediaries such as proxy servers and firewalls as they travel from the browser to Cognos 8 components. Some intermediaries modify the information that Cognos 8 components use to calculate the cookie domain, and Cognos 8 components then cannot set cookies. The usual symptom of this problem is that users are repeatedly prompted to log on. To avoid this problem, configure the cookie domain.

To set the correct value for the cookie domain, use the format and value that represents the widest coverage for the host.

Host	Format for domain	Example
computer or server	computer or server name (no dots)	mycompany
suffix is .com, .edu, .gov, .int, .mil, .net, or .org	*.name.suffix* (two dots)	.mycompany.com

Host	Format for domain	Example
other	*.name1.name2.suffix* (three dots)	.travelinfo.co.nz

Steps

1. On each Content Manager computer, start Cognos Configuration.
2. From the **Actions** menu, click **Edit Global Configuration**.
3. Click the **General** tab.
4. Click in the **Value** column under **Cookie Settings** for each property that you want to change and specify the new value.

   If you leave the **Domain** property blank, the dispatcher derives the domain from the host name of the request.
5. Click **OK**.

Changing the Gateway

To improve Web server performance, you can configure Cognos 8 to use alternate gateways that replace the default CGI program. You can use one of the following gateways:

- Microsoft Internet Application Programming Interface (ISAPI) for Microsoft Internet Information Services on Windows
- Apache Web Server module
- Servlet Gateway Java application for application servers

There is no additional Web server configuration required to use ISAPI.To access Cognos 8 components using ISAPI, in Cognos Configuration, change the **cognos.cgi** portion of the Gateway URI property to **cognosisapi.dll**. Then specify the ISAPI URI, **http://host_name/cognos8/isapi**, in your browser.

Before you change the gateway, we recommend that you first ensure that the default CGI gateway and your configuration work in your environment.

Configure the Gateway for Cognos Apache Web Server Module

Cognos 8 provides two Apache modules. The Cognos Apache module requires Apache Server 1.3.x and the Cognos Apache 2 module requires Apache Server 2.0.x.

Steps

1. Stop Apache Web Server.

2. Append the *c8_location*/cgi-bin directory to the appropriate environment variable:
   - On Solaris or Linux, LD_LIBRARY_PATH
   - On HP-UX,

     For Apache 1.3, SHLIB_PATH

     For Apache 2.0, SHLIB_PATH and LD_LIBRARY_PATH
   - On AIX, LIBPATH
3. On HP-UX PA-RISC, do the following:
   - Ensure that the LD_PRELOAD environment variable contains /usr/lib/libcl.2.
   - For Apache 1.3, set the COG_CGIBIN_DIR environment variable to *c8_location*/cgi-bin.
4. Go to the *Apache_installation*/conf directory.
5. Open the httpd.conf file in an editor.
6. Add the following to the end of the load module list:

   LoadModule cognos_module "*c8_location*/cgi-bin/*module_name*"

   where *module_name* is as follows:

Operating system	Apache 1.3 module	Apache 2.0 module
Windows	mod_cognos.dll	mod2_cognos.dll
Solaris, AIX	mod_cognos.so	mod2_cognos.so
HP-UX PA-RISC	mod_cognos.sl	mod2_cognos.sl
HP-UX IA, Linux	(not supported)	mod2_cognos.s0

7. For Apache 1.3, add the following to the end of the add module list:

   AddModule mod_cognos.cpp
8. Add the following to the aliases section:

```
ScriptAlias /cognos8/cgi-bin "c8_location/cgi-bin"
Alias /cognos8 "c8_location/webcontent"
<Directory "c8_location/webcontent">
Options Indexes MultiViews
</Directory>
```

   The `<Directory>` directive is optional.

   Tip: Ensure that you define the cognos8/cgi-bin alias before the cognos8 alias.
9. Add the following to the server status reports section:

```
<Location /cognos8/cgi-bin/cognos_module>
  SetHandler cognos-handler
```

```
</Location>
```

10. To enable the gateway diagnostic page, add the following to the server status reports section:

```
<Location /cognos8/cgi-bin/diag_cognos_module>
  SetHandler cognos-handler
</Location>
```

    The `diag_` string is required.

11. For Apache 1.3, on Windows, Solaris, and AIX, add the following to the user directory section:

```
<IfModule mod_cognos.cpp>
  CGIBinDir "c8_location/cgi-bin"
</IfModule>
```

12. For Apache 2.0, add the following to the user directory section:

```
<IfModule mod_cognos.c>
  CGIBinDir "c8_location/cgi-bin"
</IfModule>
```

13. Save and close the file.

14. For Apache 2.0, on HP-UX, enable searching for LD_LIBRARY_PATH by running the following command in the *Apache_installation*/bin directory:

    chatr +s enable +b enable httpd

15. Start Apache Web Server.

16. In Cognos Configuration, configure the **Gateway URI** property to use the apache_mod gateway:

    http://*host_name:port*/cognos8/cgi-bin/*filename*

    where *filename* matches the name that you used in step 9.

Configure the Servlet Gateway

If you configure the Cognos Servlet Gateway to run on a supported application server, your environment does not require a Web server. The application server and the Cognos Servlet Gateway replace the functions provided by a Web server and other Cognos gateways.

Before you build and deploy the Cognos Servlet Gateway, ensure the following:

- The application server is installed and running on each computer where the servlet gateway is to be installed.
- Cognos 8 Gateway components are installed (p. 93) on the same system as the application server.
- The Cognos 8 dispatcher and Content Manager components are installed and running in the environment.
- The application server user account has full access permissions for the Cognos installation.

  We recommend that you create a new UNIX or Linux group named cognos8. This group must contain the user that starts the application server and the user that owns the Cognos files. Change the group ownership of the Cognos files to the cognos8 group, and change the file permissions for all Cognos files to GROUP READABLE/WRITABLE/EXECUTABLE. For

simplicity, you can also use the application server user account to install and run Cognos components.

To set up the Cognos Servlet Gateway to run on your application server, do the following:

- Create a separate JVM instance, if necessary.

  If you plan to run Cognos 8 and the Cognos Servlet Gateway on the same application server, the servlet gateway must be deployed to a separate JVM instance.
- Check that Cognos components are properly set up.
- Set environment variables.
- Update the Java environment.
- Configure Cognos Servlet Gateway to run on the application server.
- Change the application server startup script, if necessary.
- Change the Cognos dispatcher properties file, if using Oracle Application Server.
- Configure application server properties and deploy Cognos Servlet Gateway.
- Enable SSL, if required.
- Configure the Web server.

You can then access Cognos 8 components using the Cognos Servlet Gateway, by entering the gateway URI. For example,

http[s]:*host_name:port*/ServletGateway

The Cognos Servlet Gateway URI is case-sensitive.

Configuring Cognos 8 to Work with Other Cognos Products

Some Cognos products provide functionality that is not available in Cognos 8. You can continue to use these products in the same environment. Additional configuration tasks may be required to ensure that Cognos 8 can access objects that were created using other Cognos products. Additional requirements for access depend on how you choose to run the two products.

Enable Scheduled Reports and Agents for Cognos Planning Contributor Data Sources

To run scheduled reports and agents, which are based on Cognos Planning Contributor data sources, you must specify a shared, secret password. This helps to ensure secure communication between Cognos 8 servers and Contributor Data Server.

Steps

1. On the Report Server computer, start Cognos Configuration.

2. In the **Explorer** window, click **Data Access**, **Cognos Planning**, **Contributor Data Server**.
3. In the **Properties** window, click the **Value** box next to the **Signature password** property and then click the edit button when it appears.
4. In the **Value - Signature Password** dialog box, type the password that will be digitally signed.

   The password is case-sensitive and must match the **Signature password** property that you configure in Cognos Series 7, Configuration Manager, **Cognos Planning/Cognos 8 - Contributor Data Server/General** properties.
5. From the **File** menu, click **Save**.

A digital signature, based on the password, is created. The digital signature is encoded by Cognos 8 and decoded by Contributor Data Server.

Chapter 9: Configuring Cognos 8 Go! Office

Cognos 8 Go! Office is automatically installed with all Cognos 8 server products, except for Cognos 8 Metrics Manager.

To use Cognos 8 Go! Office, you must perform some or all of the configuration tasks described below, depending on your environment.

Deploying Cognos 8 Go! Office to Client Computers

Cognos 8 Go! Office uses Microsoft .NET Framework to allow users to interact with server-based components. Microsoft .NET Framework and the required updates are downloaded and installed by the setup file when you install Cognos 8 Go! Office. The setup file must be run on all user computers.

For a list of supported versions of Microsoft .NET Framework, view the Cognos Global Customer Services Web site (http://support.cognos.com).

To deploy Cognos 8 Go! Office with PowerPlay, you can configure gateway mappings so that Cognos 8 Go! Office users can access PowerPlay reports that reside on a PowerPlay server. You can also configure the size of report that can be imported from Cognos 8 to Cognos 8 Go! Office. For more information about gateway mappings and report size limits, see the *Administration and Security Guide*.

Configuration Tasks for Cognos 8 Go! Office

Use the following checklist to configure Cognos 8 Go! Office:

- ❑ Create a virtual directory for Cognos 8 Go! Office.
- ❑ Update the recognized MIME types for the Web server, if required.
- ❑ Enable secure sockets layer support, if required.
- ❑ Enable anonymous access, if required.
- ❑ Deploy Cognos 8 Go! Office to client environments.

Create a Virtual Directory for Cognos 8 Go! Office

You must set up a virtual directory, also known as a Web alias, for the directory that contains the HTML and Web files for Cognos 8 Go! Office. For some Web servers, you must also enable directory browsing for the virtual directory and set the execute permissions property.

Only the steps for Microsoft Internet Information Services (IIS) are included below. You must set up the equivalent virtual directory and directory properties if you use another Web server.

For Apache Web Server, ensure that you define the cognos8/cgi-bin alias before the cognos8 alias in the httpd.conf file located in the *Apache_installation*/conf directory. The cognos8/cgi-bin alias must be defined as a ScriptAlias.

Steps for IIS

1. In the Internet Information Services management console, locate the virtual directory that you created for Cognos 8.

   If there is no virtual directory for Cognos 8, see "Configure the Web Server " (p. 132).

2. Right-click the Cognos 8 virtual directory and click **New**, **Virtual Directory**.
3. Follow the steps in the wizard to specify an alias named coc and the location of the Web content for Cognos 8 Go! Office, such as *c8_location*/webcontent/coc.
4. Right-click the coc directory, and click **Properties**.
5. On the **Virtual Directory** tab, do the following:
   - Select the **Directory Browsing** check box.
   - In the **Execute Permissions** box, click **Scripts only**.
6. Click **OK**.

Update the Recognized Content Types for the Web Server

For some Web servers, such as Microsoft Internet Information Services (IIS) version 6.0 or a Windows 2003 Server, you may have to add the extension .config to the recognized content, or MIME, types.

Only the steps for IIS are included below. You may have to set the equivalent for your Web server.

Steps for IIS

1. In the Internet Information Services (IIS) Manager, locate the *c8_location*\webcontent\coc directory.
2. Right-click the COC directory, and click **Properties**.
3. On the **HTTP Headers** tab, click **File Types**.
4. Click **New Type**.
5. In the **Associated Extension** box, type

   .config

6. In the **Context type** (**MIME**) box, type

   text/xml

7. Click **OK**.

Enable SSL Support for the HTTPS Interface to PowerPlay

If your environment includes Cognos Series 7 PowerPlay Enterprise Server and you are using the HTTPS interface to access PowerPlay, you must enable Secure Sockets Layer (SSL) support. To enable SSL support for the PowerPlay gateway and the Cognos 8 dispatcher, you must define a password for the Cognos 8 key store and then create and store the Web server Certificate Authority (CA) certificate in the Cognos 8 key store.

Steps to Enable SSL Support

1. Save the Web server CA certificate in the *c8_location*\bin directory and name it ca.cer.
2. If you did not define a password for the Cognos 8 key store, do it now in Cognos Configuration:
   - In the **Explorer** window, click **Cryptography**, **Cognos**.
   - In the **Properties** window, under **Certificate Authority settings**, set the **Certificate Authority key store password**.
   - From the **File** menu, click **Save**.
   - From the **Actions** menu, click **Restart**.
3. From the command line, go to the *c8_location*\bin directory.
4. Set the JAVA_HOME environment variable to the Java Runtime Environment location used by the application server running Cognos 8.

   The following examples assume that the default Tomcat application server is being used:
   - For Microsoft Windows, type

     set JAVA_HOME=*c8_location*\bin\jre*version*
   - For UNIX Cshell, type

     setenv JAVA_HOME *c8_location*/bin/jre/*version*
5. From the same command line, run the certificate tool:
   - For Microsoft Windows, type

     ThirdPartyCertificateTool.bat -T -i -r ca.cer -k ..\configuration\signkeypair\jCAKeystore -p *keystore password*
   - For UNIX, type

     ThirdPartyCertificateTool.sh -T -i -r ca.cer -k ../configuration/signkeypair/jCAKeystore-p

If required, you can now install the CA certificate on the client.

Steps to Install the CA Certificate on the Client Workstation

1. Retrieve the CA certificate from the issuing authority.

The file has a .cer extension. This is not the same certificate as the one used by the Web server. It is the certificate for the issuing authority itself.

2. Double-click the .cer file, click **Install Certificate**, and then click **Next**.
3. Click **Place all certificates in the following store**.
4. Click **Browse**, click **Trusted Root Certification Authorities**, and then click **Next**.
5. Click **Finish**.

Enable Anonymous Access for PowerPlay

When using single signon with Microsoft Internet Information Services (IIS), anonymous access must be enabled for portal users to access Cognos 8 Go! Office documents that are based on PowerPlay reports.

If necessary, a second PowerPlay gateway can be used to provide anonymous access for Cognos 8 Go! Office. For more information, see the topic about specifying gateway mappings in the *Administration and Security Guide*.

Steps

1. On each computer where Content Manager is installed, start Cognos Configuration.
2. In the **Explorer** window, under **Security**, **Authentication**, click **Cognos**.
3. In the **Properties** window, click the box next to the **Allow anonymous access** property and then click **True**.
4. From the **File** menu, click **Save**.

Deploying Cognos 8 Go! Office Client

After Cognos 8 is installed and configured, you can deploy Cognos 8 Go! Office to client workstations.

Use the following checklist to guide you through the deployment process:

- ❑ Install .NET Framework and Cognos 8 Go! Office.
- ❑ Set the macro security level for Microsoft Office XP, if required.
- ❑ Test Cognos 8 Go! Office.

Install Microsoft .NET Framework and Cognos 8 Go! Office

To install Microsoft .NET Framework and Cognos 8 for Microsoft Office, you run a setup.exe file from a central LAN location. The file installs and updates your Microsoft .NET Framework, installs

the Primary Interop Assemblies (PIAs) that are required by Microsoft Office, and installs the Cognos 8 for Microsoft Office components.

When you install Microsoft .NET Framework in a non-English operating system, Microsoft .NET error messages, shortcuts, and utilities appear in English.

For a language other than English, you can apply the Microsoft .NET Framework Language Pack to view error messages, shortcuts, and utilities in your language. For example, if your operating system is French and you installed Microsoft .NET Framework, you must also apply Microsoft .NET French Language Pack. You can download .NET Framework Version 2.0 Language Pack from http://www.microsoft.com/downloads/.

Before you update and install components, ensure that you

- have administrative privileges on the computer
- uninstalled the previous version of Cognos 8 Go! Office
- have the appropriate license to use Cognos 8 Go! Office

Steps

1. From the LAN location, run the setup.exe file.

   The installation wizard checks whether Microsoft .NET Framework is installed.

2. If the **Cognos 8 for Microsoft Office Setup** dialog box shows the License Agreement page for Microsoft .NET Framework 2.0, click **Accept**.

3. In the **Cognos 8 for Microsoft Office Setup** dialog box, click **Install**.

   If Microsoft .NET Framework is being installed, a progress dialog appears while the files are downloaded from the Microsoft download Web site and then installed. This may take several minutes.

   A progress dialog appears while the shared add-in support update for Microsoft .NET Framework is installed. When the update is complete, the Cognos 8 for Microsoft Office setup Wizard appears.

4. In the **Welcome to the Cognos 8 for Microsoft Office Setup Wizard** page of the Cognos 8 for Microsoft Office window, click **Next**.

5. In the **License Agreement** page, select **I Agree** and then click **Next**.

6. In the **Select Installation Folder** page, do the following:

   - Select the installation directory that you used for the old version, such as C:\Program Files\Cognos\Cognos Office\.
   - Select **Everyone**.

     When you select **Everyone**, all users who log on to the computer will see **Cognos 8** in the toolbar of the Microsoft Office products. If you select **Just Me**, only the user who installed Cognos 8 for Microsoft Office will see **Cognos 8** in the toolbar.

   - Click **Next**.

If a dialog box appears, advising you to uninstall a previous version, follow the prompts and uninstall the previous version, and then resume the installation.

7. In the **Confirm Installation** page, click **Next**.

   The wizard installs the Cognos 8 Go! Office components.

8. In the **Installation Complete** page, click **Close**.

Set Macro Security Level for Microsoft Office XP

For Microsoft Office XP applications to run Cognos 8 Go! Office, you must set your macro security level to an appropriate level. You must set this for Microsoft Office Excel, Microsoft Office Word, and Microsoft Office PowerPoint.

Steps

1. Open your Microsoft Office XP application.
2. From the **Tools** menu, click **Macros**, and then click **Security**.
3. Choose whether to change the security level or the trusted publishers.
   - On the **Security Level** tab, click **Medium** or **Low**, and then click **OK**
   - On the **Trusted Publishers** tab, select **Trust all installed add-ins or templates**, and then click **OK**.

Test Cognos 8 Go! Office

You can test the installation of the client components by starting Cognos 8 Go! Office. Cognos 8 Go! Office starts automatically when users start Microsoft Office Word, Microsoft Office Excel, or Microsoft Office PowerPoint, or when users open a Microsoft Office file or template.

Steps

1. Start Microsoft Office Excel, Microsoft Office Word, or Microsoft Office PowerPoint or open a Microsoft Office document, workbook, or presentation.
2. Confirm that **Cognos 8** appears in the toolbar.

   If **Cognos 8** is not in the toolbar, from the **View** menu, click **Toolbars**, **Cognos 8 for Microsoft Office**.

3. To show the action pane, click **Cognos 8** in the toolbar.

   The **Cognos 8 for Office** pane appears on the right-hand side of the window. It includes a link to Cognos 8 Go! Office.

Chapter 10: Configuring Portal Services

Portal Services provides a set of Cognos portlets that you can use in Cognos Connection and in third-party portals. You can use the portlets to navigate, search, and view Cognos reports in your working environment. Other users can view Cognos information without needing to know how to use Cognos products.

For more information, see the *Administration and Security Guide*.

Portal Services is installed automatically with Cognos 8 components. In a distributed environment, it is included with the Application Tier Components. The installation includes the deployment files for

- SAP Enterprise Portal (SAP EP)
- IBM WebSphere Portal
- Plumtree Portal
- SharePoint Portal

For some deployments of Portal Services, you must modify some Portal Services property settings and prepare the Cognos environment to support the third-party portal.

When used in a third-party portal, Portal Services can authenticate users in only one namespace. If Cognos 8 components are configured with more than one namespace, you must install a separate gateway for each namespace that will be used to authenticate portal users. You must configure each gateway to use the appropriate namespace (p. 203) and then configure the deployed portlets to use that gateway.

After you configure the required properties, you must deploy the Cognos portlets to the third-party portal. For more information, see the *Administration and Security Guide*.

To use Portal Services with Cognos 8 components, do the following:

- ❑ Specify the location of the applications.xml file, if required.
- ❑ Install and test the portlets on the third-party portal.

  For more information, see the *Administration and Security Guide*.
- ❑ Configure security for the third-party portal environment.

Specify the Location of the Applications.xml File

If you use the applications.xml file as part of a custom application portlet, all Application Tier Components computers in a distributed environment must reference the same applications.xml file. If you have multiple instances of the applications.xml file, they must be identical.

Note: The steps are required only if you want to use the Extended Applications portlet, which is included with the Cognos 8 software development kit.

Steps

1. On the computer where you installed the report server, start Cognos Configuration.
2. In the **Explorer** window, under **Environment**, click **Portal Services**.
3. In the **Properties** window, click the **Value** next to **Location of 'applications.xml'**.
4. Replace localhost with a valid host name or IP address and, if necessary, replace the default port number.
5. From the **File** menu, click **Save**.

You can now deploy the Cognos portlets to your portal server. For instructions, see the *Administration and Security Guide*.

Configuring Security for Portal Services

When using Portal Services in a third-party portal, you must enable single signon to provide seamless integration between the third-party portal and Cognos 8 components.

Portal Services uses single signon to authenticate users. This means that users do not have to log on to other applications separately through the portal.

You must configure a URI into Cognos 8 components for each portlet in Portal Services.

To enable security between Cognos 8 components and the third-party portal, do the following:

- ❑ Disable anonymous access to Cognos 8 components.

  If your security infrastructure requires you to use another method for single signon, use one of the following methods:

- ❑ Enable single signon for the third-party portal using shared secret.

  If your security infrastructure requires you to use another method for single signon, use one of the following methods:

  - "Enable Single Signon for WebSphere Portal Using the Application Server" (p. 252)
  - "Enable Single Signon for Plumtree Portal Using Basic Authentication" (p. 253)
  - "Enable Single Signon for Plumtree Portal Using SiteMinder" (p. 253)

- ❑ Configure Cognos 8 components for SSL access, if required.

Disable Anonymous Access to Cognos 8 Components

Portal Services uses single signon for authentication. If anonymous logon is enabled in Cognos 8 components, Portal Services logs all portal users as anonymous. You must ensure that anonymous access is disabled in Cognos 8 components for single signon in Portal Services to be successful.

However, you can test the Portal Services connections using anonymous logon to ensure that the portlets are working in the third-party portal.

If Portal Services fails to authenticate a user, the user receives an error message at the third-party portal.

Steps

1. Start Cognos Configuration.
2. In the **Explorer** window, under **Security**, **Authentication**, click **Cognos**.
3. In the **Properties** window, ensure that **Allow anonymous access** is set to **False**.
4. From the **File** menu, click **Save**.
5. Repeat steps 1 to 4 on all servers where you installed Cognos 8 components.

Enable Single Signon Using Shared Secret

You can use shared secret for single signon between Cognos portlets and Cognos 8 components. The Cognos portlets send a message that contains an encrypted version of the portal user ID. The encryption key is determined by the value of a secret character string shared between the portlets and the custom Java security provider on the Cognos server.

You can use shared secret for the third-party portal only if portal user IDs can be looked up in an NTLM, LDAP, or Cognos Series 7 authentication namespace that is shared by Cognos 8 components.

Cognos 8 components must have access to a directory server that contains user IDs for all your portal users. Using Cognos Configuration, you must configure an authentication namespace so that the portal and Cognos 8 components share the same authentication source.

You must also create a Custom Java Provider namespace to register the shared secret Java provider that is provided with Cognos 8 components. Within the portlets or iViews, you must link the portlets or iViews to the Custom Java Provider namespace within your respective portal:

- Cognos iViews (SAP EP)
- Cognos Portlet Application (WebSphere Portal)
- remote server (Plumtree Portal)
- Cognos WebPart (SharePoint Portal)

You are not required to configure access to the Portal Services Web content. However, if you deploy the portlets to a third-party portal, you can configure access to an alternate URI for Portal Services images and Web content.

Steps to Configure the Required Namespaces

1. In Cognos Configuration, configure a namespace to authenticate portal users.

   For more information, see "Configuring Cognos 8 Components to Use an Authentication Provider" (p. 255).

2. For an LDAP namespace, configure the following properties:
   - For the **Use external identity** property, change the setting to **True**.
   - For the **External identity mapping** property, set it to

     (uid=${environment("REMOTE_USER")})

3. For a Cognos Series 7 namespace, map the portal user IDs to Cognos Series 7 user IDs using OS signons.

   For more information, see the Cognos Series 7 documentation.

4. In Cognos Configuration, create and configure a Custom Java Provider namespace.
   - For the **Namespace ID** property, specify any new ID.

     For example, **cpstrusted**

     This new ID must be used in the portlet configuration settings.
   - For the **Java class name** property, type

     com.cognos.cps.auth.CPSTrustedSignon

     Java class names are case-sensitive.

5. In Cognos Configuration, under **Environment**, **Portal Services**, configure the following properties:
   - For **Trusted Signon Namespace ID**, type the namespace ID of the LDAP, NTLM, or Cognos Series 7 namespace that you configured in step 1.

     Tip: The trusted signon namespace acts as an intermediary and must be attached to a real directory-based namespace of type LDAP, NTLM, or Cognos Series 7.
   - For **Shared Secret**, type the key to be used for single signon.

     This parameter represents the authorization secret that must be shared between the Cognos portlets and the Cognos server. Consider this as a secret password. You must use the same character string when you configure the portlet application. You must use a single word as the key.

     For security reasons, we recommend you specify a non-null value.

6. Under **Environment**, for **Gateway Settings**, set the **Allow Namespace Override** property to **true**.
7. From the **File** menu, click **Save**.
8. Restart the Cognos 8 service.

Steps to Configure Access to the Portal Services Web Content

1. On the computer where you installed the Application Tier Components, start Cognos Configuration.
2. In the **Explorer** window, under **Environment**, click **Portal Services**.
3. In the **Properties** window, click the **Value** box next to **Web Content URI**.

4. Specify the host name or IP address of the gateway and a port number using the format

   host_or_IP_address:port

5. From the **File** menu, click **Save**.

Steps to Configure the Cognos iViews for SAP EP

1. Open the iView editor for each Cognos iView.
2. In the **Property Category** box, select **Show All**.
3. For the **cpsauthsecret: CPS Authorization Secret** property, enter the secret character string that you used for the Shared Secret property when you configured the Custom Java Provider namespace.
4. For the **cps: authentication namespace ID** property, enter the Custom Java Provider namespace ID.
5. For the **cpsserver: CPS Connection Server** property, enter the URL path to access Portal Services components through the gateway.

   The format of the URL is as follows:

   - For Cognos content portlets

     ***Gateway_URI*/wsrp/cps4/portlets/nav?wsdl&b_action=cps.wsdl**

     Example for a CGI gateway:

     http://*myserver*/cognos8/cgi-bin/cognos.cgi/wsrp/cps4/portlets/nav?wsdl&b_action=cps.wsdl

     Example for a servlet gateway:

     http://172.0.16.1:9500/wsrp/cps4/portlets/nav?wsdl&b_action=cps.wsdl

   - For Cognos Extended Applications

     ***Gateway_URI*/wsrp/cps4/portlets/sdk?wsdl&b_action=cps.wsdl**

     Example for a CGI gateway:

     http://*myserver*/cognos8/cgi-bin/cognos.cgi/wsrp/cps4/portlets/sdk?wsdl&b_action=cps.wsdl

     Example for a servlet gateway:

     http://172.0.16.1:9500/wsrp/cps4/portlets/sdk?wsdl&b_action=cps.wsdl

   - For Metrics Manager Watchlist portlets

     ***Gateway_URI*/wsrp/cps4/portlets/cmm?wsdl&b_action=cps.wsdl**

     Example for a CGI gateway:

     http://*myserver*/cognos8/cgi-bin/cognos.cgi/wsrp/cps4/portlets/cmm?wsdl&b_action=cps.wsdl

     Example for a servlet gateway:

http://172.0.16.1:9500/wsrp/cps4/portlets/cmm?wsdl&b_action=cps.wsdl

Steps to Configure the Cognos Portlets for WebSphere Portal

1. For each Cognos portlet application, click **Modify Parameters**.
2. For the **cps_auth_secret** property, enter the secret character string that you used for the **Shared Secret** property when you configured the Custom Java Provider namespace.
3. For the **cps_auth_namespace** property, enter the Custom Java Provider namespace ID.
4. For the **CPS Endpoint** property, enter the URL path to access Portal Services components through the gateway.

   The format of the URL is as follows:

   - For Cognos content portlets

     ***Gateway_URI*/wsrp/cps4/portlets/nav?wsdl&b_action=cps.wsdl**

     Example for a CGI gateway:

     http://*myserver*/cognos8/cgi-bin/cognos.cgi/wsrp/cps4/portlets/nav?wsdl&b_action=cps.wsdl

     Example for a servlet gateway:

     http://172.0.16.1:9500/wsrp/cps4/portlets/nav?wsdl&b_action=cps.wsdl

   - For Cognos Extended Applications

     ***Gateway_URI*/wsrp/cps4/portlets/sdk?wsdl&b_action=cps.wsdl**

     Example for a CGI gateway:

     http://*myserver*/cognos8/cgi-bin/cognos.cgi/wsrp/cps4/portlets/sdk?wsdl&b_action=cps.wsdl

     Example for a servlet gateway:

     http://172.0.16.1:9500/wsrp/cps4/portlets/sdk?wsdl&b_action=cps.wsdl

   - For Metrics Manager Watchlist portlets

     Gateway_URI/wsrp/cps4/portlets/cmm?wsdl&b_action=cps.wsdl

     Example for a CGI gateway:

     http://*myserver*/cognos8/cgi-bin/cognos.cgi/wsrp/cps4/portlets/cmm?wsdl&b_action=cps.wsdl

     Example for a servlet gateway:

     http://172.0.16.1:9500/wsrp/cps4/portlets/cmm?wsdl&b_action=cps.wsdl

Steps to Configure the Remote Server for Plumtree Portal

1. Using a plain ASCII editor, such as Notepad, edit the cpspt.properties file in the *c8_location*/cps/plumtree/webapps/gadgets/WEB-INF/classes directory.

2. Configure the following settings.

Parameter	Value
cps_endpoint	The URL to connect to the report server and extract the WSDL information. Specify the URI to the gateway. For a servlet or ISAPI gateway, replace the localhost/cognos8/cgi-bin/cognos.cgi portion with the values to target the gateway. For example, **http://host_name/cognos8/cgi-bin/cognos.isapi/wsrp/cps4/portlets/[package]?wsdl&b_action=cps.wsdl**
forward_cookies=	The names of the cookie that should be sent to the report server for single signon. Leave blank.
cps_auth_secret	The shared secret code Cognos 8 uses to encrypt an HTTP header variable that carries the user identity. This parameter represents the authorization secret that must be shared between the Cognos portlets and the Cognos 8 server. Consider this as a secret password. Use the same value that you used for **Shared Secret** in Cognos Configuration. For security reasons, we recommend you specify a non-null value.
cps_auth_namespace	The namespace ID for the Custom Java Provider.

3. Go to the *c8_location*/cps/plumtree directory and run the following build file:
   - On UNIX or Linux, **build.sh**
   - On Windows, **build.bat**

   This creates a cps-pt.war file in the *c8_location*/cps/plumtree/gadgets directory.
4. If Cognos 8 components are running using Tomcat,
   - Stop Cognos 8.
   - Copy the cps-pt.war file to the *c8_location*/webapps directory.

     Tomcat automatically expands the WAR file and starts the remote server.
   - Start Cognos 8.
5. If Cognos 8 components are running under another type of application server, copy the cps-pt.war file to the application server.

For instructions, see the administration guide for your application server.

Single signon is configured.

Steps to Configure Properties for the Cognos WebPart for SharePoint Portal

1. Using a plain ASCII editor, such as Notepad, edit the web.config file in the *drive*\Program Files\Common Files\Microsoft Shared\web server extensions\60\CONFIG directory.
2. Find the following string:

   ```
   <SSO cps_auth_namespace="" cps_auth_secret="" />
   ```

3. Set cps_auth_namespace to the namespace ID for the Custom Java Provider namespace.
4. Set cps_auth_secret to the value that you used for **Shared Secret** in Cognos Configuration.

Enable Single Signon for SAP EP with the SAP Logon Ticket

If you enable single signon with the SAP Logon Ticket, you must configure Cognos 8 components with an SAP namespace that links to an SAP BW server.

Then you must copy the certificate that was generated during SAP EP installation to the SAP BW personal security environment.

Users must have the same user ID in all SAP systems that are accessed through single signon.

Before you start, ensure that you have

- configured Cognos 8 components to use an SAP authentication source
- enabled single signon between Cognos 8 components and SAP BW
- installed the latest service packs on the SAP BW server

  Service packs can be downloaded from SAPNET.
- installed the latest hot patches for the SAP portal
- installed the Enterprise Portal plug-in that corresponds to the SAP EP release or SAP BW server

  For SAP releases earlier than 6.2, on SAPNET, download EP50_PLUG-IN for Basis 620 (SAPKINE32A). Using transaction SAINT, install SAPKINE32A.
- installed the SAP Security Library on the SAP BW servers

  From sapservX, under /general/misc/security/SAPSECU/platform, download sapsecin and sepsecu.dll and place both files in the /run directory of the SAP BW server.

To enable SSO for SAP EP, complete the procedures for single signon with SAP logon tickets in the SAP Enterprise Portal *Security Guide*.

You can now use the Cognos iViews in the SAP Enterprise Portal. For more information, see the *Administration and Security Guide*.

Enable Single Signon for SAP EP with User Mapping

If you enable single signon with user mapping, you define a Cognos data source in SAP EP. Individual users or an administrator can enter the user IDs and passwords for Cognos 8 components in the data source. You must map the users logon credentials in the data source to an LDAP or Cognos Series 7 or NTLM namespace. Portal Services iViews transmit the logon credentials to Cognos 8 components using HTTP Basic Authentication.

Steps to Prepare the Environment

1. Configure the gateway URI that will be used by Portal Services to require authentication using HTTP Basic Authentication.

   For information about configuring a URL to use HTTP Basic Authentication, see the documentation for the gateway or for your Web server.

2. Adjust the iView configuration to access the secure URL.

   For information, see the documentation for your Web server.

3. In Cognos Configuration, configure a namespace to authenticate portal users.

4. If you use an LDAP namespace, configure the following properties:

   - For the **Use external identity** property, change the setting to **True**.
   - For the **External identity mapping** property, set it to

     (uid=${environment("REMOTE_USER")})

Steps to Create the Data Source and Map the Users

1. In the SAP portal, ensure that the following properties are configured for the data source in the /PortalContent/other_vendors/every_user/com.cognos.pct.c8/systems/Cognos 8 directory:

   - **Logon Method** = UIDPW
   - **server name** = the name of the Cognos server
   - **port number** = port number of the gateway
   - **Protocol of Target system** = HTTP
   - **User Mapping Type** = admin,user
   - **system alias** (Create a system alias)

   For more information, see the SAP Enterprise Portal *Administration Guide*.

2. For each Cognos iView, enable user mapping for the data source by entering the name of the system alias at the iView level, in an attribute called **CPS: User Mapping Datasource**.

   For more information, see the SAP Enterprise Portal *Administration Guide*.

3. For each Cognos iView, set the **CPS: Authentication Namespace ID** property to the namespace that you want to use for authentication.

4. Register the Cognos credentials for the portal users.

   Users can enter their own user IDs and passwords.

   For more information, see the SAP Enterprise Portal *Administration Guide*.

We recommend that you enable secure communication between SAP EP and Cognos 8.

You can now use the Cognos iViews in the SAP Enterprise Portal. For more information, see the *Administration and Security Guide*.

Enable Secure Communication Between SAP EP and Cognos 8 Components

A secure connection, using SSL, is not required between SAP EP and Cognos 8 components. It is more important if you enabled single signon with user mapping.

The SSL security supported by SAP uses encryption above 56 bits. By default, Cognos 8 components use an encryption algorithm up to 56 bits. Cognos provides an enhanced encryption module as a complementary product. To enable SSL, you must purchase and install the Enhanced Encryption Module for OpenSSL on top of Cognos 8 components. For more information, see the Cognos Enhanced Encryption Module for OpenSSL *Installation and Configuration Guide*.

To enable SSL between SAP EP and Cognos 8 components, see your SAP EP security documentation.

After SSL is enabled, edit properties for the all iViews so that the **cpsserver: CPS Connection Server** property uses https instead of http.

You can now use the Cognos portlets in the SAP Enterprise Portal. For more information, see the *Administration and Security Guide*.

Enable Single Signon for WebSphere Portal Using the Application Server

The Portal Services portlets can use the Active Credentials objects provided by WebSphere Portal to connect to Cognos 8 components. Portal Services supports the following Active Credentials objects: HttpBasicAuth, LtpaToken, SiteMinderToken, and WebSealToken.

Credentials for the portal user are passed to the gateway using this object. For more information about Active Credential objects, see the documentation for IBM WebSphere Portal.

To use application server single signon, see the documentation for IBM WebSphere Application Server.

For information about SSL for Cognos 8 components on a WebSphere Application Server, see "Configuring the SSL Protocol" (p. 211).

After single signon is set up, you can use the Cognos portlets in the WebSphere Portal. For more information, see the *Administration and Security Guide*.

Enable Single Signon for Plumtree Portal Using Basic Authentication

You can configure a portlet in Plumtree Portal to send the username and password as an HTTP Basic authentication header. The header can be used with an NTLM, LDAP, or Cognos Series 7 authentication namespace to provide single signon.

Steps

1. In Cognos Configuration, configure a namespace to authenticate portal users.
2. Install an alternate CGI or ISAPI or servlet gateway in Cognos 8.
3. Configure the gateway.
4. In the administration console of the Web server, configure the virtual directories to access the gateway.

   For more information, see the documentation for your Web server.
5. Configure the Plumtree remote server to access Cognos 8:
   - Edit the cpspt.properties file in the *c8_location*/cps/plumtree/webapps/gadgets/WEB-INF/classes directory.
   - Change the cps_endpoint property to indicate the URL of the gateway.

     For a CGI gateway, you can use the default setting if the gateway and the remote server are on the same computer. Otherwise, replace the localhost portion with **host_name:port**

     For a servlet or ISAPI gateway, replace the localhost/cognos8/cgi-bin/cognos.cgi portion with the values to target the gateway.

     For example,

     http://*host_name*:*port*/cognos8/cgi-bin/cognos.isapi/wsrp/cps4/portlets/[package]?wsdl&b_action=cps.wsdl
   - Set the **cps_auth_namespace** property to the namespace that you want to use for authentication.

Enable Single Signon for Plumtree Portal Using SiteMinder

If you use eTrust SiteMinder to provide single signon in your security infrastructure, you can also use it for single signon with Plumtree Portal.

You must configure a SiteMinder authentication namespace in Cognos 8. Plumtree Portal sends the SiteMinder active authentication token to the remote server, which sends the token to the Cognos 8 gateway.

Steps

1. In Cognos Configuration, configure a SiteMinder authentication namespace.

   For instructions, see "Configuring Cognos 8 Components to Use eTrust SiteMinder" (p. 283).

2. Configure the remote server to forward the authentication token:
   - Edit the cpspt.properties file in the *c8_location*/cps/Plumtree/webapps/gadgets/WEB-INF/classes directory.
   - Change the forward_cookies property to include the name of the active authentication token that SiteMinder provides.
   - Change the cps_endpoint property to indicate the URL of the gateway.

     For a CGI gateway, you can use the default setting if the gateway and the remote server are on the same computer. Otherwise, replace the localhost portion with ***host_name*:*port***.

     For a servlet or ISAPI gateway, replace the localhost/cognos8/cgi-bin/cognos.cgi portion with the values to target the gateway.

     For example,

     http://*host_name*:*port*/cognos8/cgi-bin/cognos.isapi/wsrp/cps4/portlets/[package]?wsdl&b_action=cps.wsdl
   - Change the **cps_auth_namespace** property to the namespace that you want to use for authentication.

Chapter 11: Configuring Cognos 8 Components to Use an Authentication Provider

Cognos 8 components run with two levels of logon: anonymous and authenticated. By default, anonymous access is enabled.

You can use both types of logon with your installation. If you choose to use only authenticated logon, you can disable anonymous access.

For authenticated logon, you must configure Cognos 8 components with an appropriate namespace for the type of authentication provider in your environment. You can configure multiple namespaces for authentication and then choose at run time which namespace you want to use. For more information, see the *Administration and Security Guide*.

If you upgraded from ReportNet and Cognos 8 detects a previously configured namespace that is no longer configured, the unconfigured namespace appears in the list of authentication providers in the Administration portal. You can configure the namespace if you still require the user account information. Otherwise, you can delete the namespace. For information about deleting the namespace, see the *Administration and Security Guide*.

Also, when upgrading from one version to another, you must use the same authentication namespace for both versions. Otherwise, the new version may not contain the same policies, users, roles, and groups.

Cognos 8 components support the following types of servers as authentication sources:

- Active Directory Server
- Cognos Series 7
- Custom Authentication Provider
- LDAP
- eTrust SiteMinder
- NTLM
- SAP

If you use more than one Content Manager computer, you must configure identical authentication providers on each Content Manager computer. This means that the type of authentication provider you select and the way you configure it must be identical on all computers for all platforms. The configuration must contain information that is accessible by all Content Manager computers.

When Cognos 8 is installed on a single Linux computer, or when Content Manager is installed on a Linux computer, Cognos 8 can be configured to use only LDAP V3-compliant directory servers and custom providers as authentication sources.

Some authentication providers require libraries external to the Cognos 8 environment to be available. If these libraries are not available on Linux, the authentication provider cannot be initialized.

If you want to configure one of the following as your authentication source, you must install Content Manager on a non-Linux computer:

- Cognos Series 7 namespace
- Active Directory Server
- NTLM
- eTrust SiteMinder
- SAP BW

If you enable security, you must configure security settings immediately after you complete the installation and configuration process. For more information, see the *Administration and Security Guide*.

Important: We recommend that you do not disable security after you enable it. If you delete a namespace, the user preferences, My Folders, and My Pages entries are permanently lost. Existing permission settings will refer to users, groups or roles that no longer exist. While this does not affect how the permissions work, a user administering the permission settings may see "unknown" entries. Because these entries refer to users, groups, and roles which no longer exist, you can safely delete them.

After you configure an authentication provider for Cognos 8 components, you can enable single signon between your authentication provider environment and Cognos 8 components. This means that a user logs on once and can then switch to another application without being asked to log on again.

To use an authentication provider and to require users to authenticate:

- ❑ Disable anonymous access, if required.
- ❑ Configure Cognos 8 components to use an authentication provider.

Disable Anonymous Access

By default, Cognos 8 components do not require user authentication. Users can log on anonymously.

If you want to use authenticated logon only, you can use Cognos Configuration to disable anonymous access.

Steps

1. On each Content Manager computer, start Cognos Configuration.
2. In the **Explorer** window, under **Security**, **Authentication**, click **Cognos**.

   The Cognos resource represents the Cognos namespace. The Cognos namespace stores information about Cognos groups, such as the Anonymous User, contacts, and distribution

lists, and refers to objects in other security namespaces. For more information, see the *Administration and Security Guide*.

3. In the **Properties** window, click the box next to the **Allow anonymous access** property and then click **False**.
4. From the **File** menu, click **Save**.

Now, users are required to provide logon credentials when they access Cognos resources.

Restrict User Access to the Cognos Namespace

Access can be restricted to users belonging to any group or role defined in the Cognos built-in namespace. By default, all users belong to several built-in groups or roles. To restrict access, you must:

- enable the property to restrict access
- remove the Everyone group from the Cognos built-in roles and groups
- ensure that authorized users belong to at least one Cognos role or group

Steps

1. On each Content Manager computer, start Cognos Configuration.
2. In the **Explorer** window, under **Security**, click **Authentication**.
3. In the **Properties** window, change the value of **Restrict access to members of the built-in namespace** to **True**.
4. From the **File** menu, click **Save**.

You must now use the portal to remove the Everyone group from the Cognos built-in roles and groups and then ensure that authorized users belong to at least one Cognos built-in role or group.

For information about adding or removing members of a Cognos group or role, see the *Administration and Security Guide*.

Configuring Cognos 8 Components to Use Active Directory Server

If you install Content Manager on a Windows computer, you can configure Active Directory as your authentication source using an Active Directory namespace.

If you install Content Manager on a UNIX computer, you must instead use an LDAP namespace to configure Active Directory as your authentication source. If you install Content Manager on Windows and UNIX computers, you must use an LDAP namespace to configure Active Directory on all Content Manager computers. When you use an LDAP namespace to authenticate against Active Directory Server, you are limited to LDAP features only. You do not have access to Active

Directory features such as advanced properties for domains (p. 261) and single signon using Kerberos delegation (p. 262).

If you install Content Manager on a Linux computer, the same restrictions apply as for UNIX. You must use an LDAP namespace to configure Active Directory as your authentication source.

For more information, see "Configure an LDAP Namespace for Active Directory Server" (p. 271).

If you want to use Microsoft SQL Server or Microsoft Analysis Server as a data source and use single signon for authentication, you must use Active Directory as your authentication source.

You cannot connect to the Active Directory Global Catalog, which is a caching server for Active Directory Server. If the connection uses port 3268, you must change it. By default, Active Directory Server uses port 389.

To use an Active Directory Server namespace and to set up single signon, do the following:

- Configure Cognos 8 components to use an Active Directory Server namespace
- Enable secure communication to the Active Directory Server, if required
- Enable single signon between Active Directory Server and Cognos 8 components

Configure an Active Directory Namespace

You can use Active Directory Server as your authentication provider.

You also have the option of making custom user properties from the Active Directory Server available to Cognos 8 components.

For Cognos 8 to work properly with Active Directory Server, you must ensure that the Authenticated users group has Read privileges for the Active Directory folder where users are stored.

If you are configuring an Active Directory namespace to support single signon with a Microsoft SQL Server or Microsoft Analysis Server data source, the following configuration is required:

- The Cognos 8 gateway must be installed on an IIS Web server that is configured for Windows Integrated Authentication.
- The gateway must be assigned to the local intranet Web site in your Web browser.
- Content Manager must be installed on a Windows 2000 or Windows 2003 server.
- Content Manager, the report server (Application Tier Components), IIS Web server, and the data source server (Microsoft SQL Server or Microsoft Analysis Server) must belong to the Active Directory domain.
- The data source connection for Microsoft SQL Server or Microsoft Analysis Server must be configured for **External Namespace** and that namespace must be the Active Directory namespace.

For more information about data sources, see the *Administration and Security Guide*.

Steps

1. On every computer where you installed Content Manager, open Cognos Configuration.

2. In the **Explorer** window, under **Security,** right-click **Authentication**, and then click **New resource**, **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the appropriate namespace and then click **OK**.

   The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.
5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
6. Specify the values for all other required properties to ensure that Cognos 8 components can locate and use your existing authentication provider.
7. Specify the values for the **Host and port** property.

   To support Active Directory Server failover, you can specify the domain name instead of a specific domain controller. For example, use *mydomain*.com:389 instead of dc1.*mydomain*.com:389.
8. If you want to be able to search for details when authentication fails, specify the user ID and password for the **Binding credentials** property.

   Use the credentials of an Active Directory Server user who has search and read privileges for that server.
9. From the **File** menu, click **Save**.
10. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

Cognos 8 loads, initializes, and configures the provider libraries for the namespace.

Make Custom User Properties for Active Directory Available to Cognos 8 Components

You can use arbitrary user attributes from your Active Directory Server in Cognos 8 components. To configure this, you must add these attributes as custom properties for the Active Directory namespace.

The custom properties are available as session parameters through Framework Manager. For more information about session parameters, see the Framework Manager *User Guide*

The custom properties can also be used inside command blocks that are used to configure Oracle sessions and connections. The command blocks can be used with Oracle light-weight connections and virtual private databases. For more information, see the *Administration and Security Guide*.

Steps

1. On every computer where you installed Content Manager, open Cognos Configuration.

2. In the **Explorer** window, under **Security**, **Authentication**, click the Active Directory namespace.
3. In the **Properties** window, click in the **Value** column for **Custom properties** and click the edit button.
4. In the **Value - Custom properties** window, click **Add**.
5. Click the **Name** column and enter the name you want Cognos 8 components to use for the session parameter.
6. Click the **Value** column and enter the name of the account parameter in your Active Directory Server.
7. Repeat steps 4 to 6 for each custom parameter.
8. Click **OK**.
9. From the **File** menu, click **Save**.

Enabling Secure Communication to the Active Directory Server

If you are using an SSL connection to the Active Directory Server, you must copy the certificate from the Active Directory Server to the Content Manager computer.

Steps

1. On every Content Manager computer, use your Web browser to connect to the Active Directory Server and copy the CA root certificate to a location on the Content Manager computer.
2. Add the CA root certificate to the certificate store of the account that you are using for the current Cognos session:
   - If you are running the Cognos session under a user account, use the same Web browser as in step 1 to import the CA root certificate to the certificate store for your user account.

     For information, see the documentation for your Web browser.
   - If you are running the Cognos session under the local computer account, use Microsoft Management Console (MMC) to import the CA root certificate to the certificate store for the local computer.

     For information, see the documentation for MMC.
3. In Cognos Configuration, restart the service:
   - In the **Explorer** window, click **Cognos 8 service**, **Cognos 8**.
   - From the **Actions** menu, click **Restart**.

Include or Exclude Domains Using Advanced Properties

When you configure an authentication namespace for Cognos 8, users from only one domain can log in. By using the Advanced properties for Active Directory Server, users from related (parent-child) domains and unrelated domain trees within the same forest can also log in.

Authentication in One Domain Tree

If you set a parameter named chaseReferrals to true, users in the original authenticated domain and all child domains of the domain tree can log in to Cognos 8. Users above the original authenticated domain or in a different domain tree cannot log in.

Authentication in All Domain Trees in the Forest

If you set a parameter named MultiDomainTrees to true, users in all domain trees in the forest can log in to Cognos 8.

Steps

1. On every computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security**, **Authentication**, click the Active Directory namespace.
3. In the **Properties** window, specify the **Host and port** property:
   - For users in one domain, specify the host and port of a domain controller for the single domain.
   - For users in one domain tree, specify the host and port of the top-level controller for the domain tree.
   - For users in all domain trees in the forest, specify the host and port of any domain controller in the forest.
4. Click in the Value column for **Advanced properties** and click the edit button.
5. In the **Value - Advanced properties** window, click **Add**.
6. Specify two new properties, **chaseReferrals** and **MultiDomainTrees**, with the following values:

Authentication for	chaseReferrals	MultiDomainTrees
One domain	False	False
One domain tree	True	False
All domain trees in the forest	True	True

7. Click **OK**.
8. From the **File** menu, click **Save**.

Enabling Single Signon Between Active Directory Server and Cognos 8 Components

By default, the Active Directory provider uses Kerberos delegation and integrates with the IIS Web server for single signon if Windows integrated authentication (formerly named NT Challenge Response) is enabled on the IIS Web server.

If Windows integrated authentication is enabled, you are not prompted to reenter authentication information when accessing Cognos content that is secured by the Active Directory namespace.

If you do not want Kerberos delegation, the provider can be configured to access the environment variable REMOTE_USER to achieve single signon. You must set the advanced property singleSignOnOption to the value IdentityMapping. You must also specify bind credentials for the Active Directory namespace. Microsoft sets REMOTE_USER by default when you enable Windows integrated authentication. If Kerberos authentication is bypassed, single signon to Microsoft OLAP (MSAS) data sources will not be possible.

Steps for Single Signon Using Kerberos Delegation

1. Set up Windows integrated authentication on the IIS Web server.
2. Install Content Manager on a computer that is part of the domain, for the active and standby Content Manager computers.
3. Set up the computers, or the user account under which Content Manager runs, to be trusted for delegation.

   When setting up the computers using the Active Directory user tool, do not select the **Account** attribute, which is sensitive and cannot be delegated.

Steps for Single Signon Using REMOTE_USER

1. On every computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security**, **Authentication**, click the Active Directory namespace.
3. Click in the **Value** column for **Advanced properties** and then click the edit button.
4. In the **Value - Advanced properties** dialog box, click **Add**.
5. In the **Name** column, type **singleSignOnOption**
6. In the **Value** column, type **IdentityMapping**.
7. Click **OK**.
8. Click in the **Value** column for **Binding credentials**, and then click the edit button.
9. In the **Value - Binding credentials** dialog box, specify a user ID and password and then click **OK**.

The Active Directory provider now uses REMOTE_USER for single signon.

Tip: To switch back to Kerberos delegation, edit **Advanced properties** and, in the **Value** column, type **KerberosAuthentication**.

Configuring Cognos 8 to Use Cognos Series 7 Namespace

You can configure Cognos 8 components to use a Cognos Series 7 namespace as the authentication provider. Users will be authenticated based on the authentication and signon configuration of the Cognos Series 7 namespace.

A Cognos Series 7 namespace is required if you want to use Cognos Series 7 PowerCubes and Transformer models in Cognos 8. The namespace must be configured before you load the Transformer models.

If you want to configure a Cognos Series 7 namespace as your authentication source, you must install Content Manager on a computer that supports Cognos Series 7.

Note: You cannot use a Cognos Series 7 Local Authentication Export (LAE) file for authentication with Cognos 8 components.

You can configure Cognos 8 components to use multiple Cognos Series 7 authentication providers. We recommend that all Cognos Series 7 namespaces use the same primary Cognos Series 7 Ticket Server. Otherwise, you may receive errors or be prompted for authentication more than once.

If you change the configuration information stored in the directory server used for Cognos Series 7, you must restart the Cognos 8 service before the changes take effect in the Cognos installation.

A user must be in at least one Access Manager user class to be able to log on to Cognos 8 components.

To use a Cognos Series 7 namespace and to set up single signon, do the following:

- Configure Cognos 8 to use a Cognos Series 7 namespace
- Enable secure communication to the directory server used by the Cognos Series 7 namespace, if required
- Enable single signon between Cognos Series 7 and Cognos 8

Configure a Cognos Series 7 Namespace

You can configure Cognos 8 to use one or more Cognos Series 7 namespaces for authentication.

Steps

1. On every computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and then click **New resource**, **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the appropriate namespace and then click **OK**.

The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.

5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
6. Specify the values for all other required properties to ensure that Cognos 8 components can locate and use your existing authentication provider.

   If your Series 7 namespace version is 16.0, ensure that the **Data encoding** property is set to **UTF-8**. In addition, the computers where Content Manager is installed must use the same locale as the data in the Series 7 namespace.

   The host value can be a computer name or an IP address. If you are publishing from PowerPlay Enterprise Server to Cognos 8, you must use the same value format that is used in Cognos Series 7 Configuration Manager for the location of the directory server. For example, if the computer name is used in Cognos Series 7 Configuration Manager, the computer name must also be used in Cognos Configuration for Cognos 8.
7. If your namespace environment includes version 15.2 of the Series 7 namespace, you must disable the **Series7NamespacesAreUnicode** setting.
   - In the **Properties** window, in the **Advanced Properties** value, click the edit button.
   - In the **Value - Advanced properties** window, click **Add**.
   - In the **Name** box, type **Series7NamespacesAreUnicode**.
   - In the **Value** box, type **False**, and then click **OK**.
8. In the **Properties** window, under **Cookie settings**, ensure that the **Path**, **Domain**, and **Secure flag enabled** properties match the settings configured for Cognos Series 7.
9. From the **File** menu, click **Save**.
10. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

Enabling Secure Communication to the Directory Server Used by the Series 7 Namespace

If you are using an SSL connection to the Directory Server used by the Cognos Series 7 namespace, you must copy the certificate from the Directory Server to each Content Manager computer.

For more information, see the Cognos Access Manager *Administrator Guide* and the documentation for your Directory Server.

Enabling Single Signon Between Cognos Series 7 and Cognos 8

If your Cognos Series 7 namespace has been configured for integration with your external authentication mechanisms for single signon, the Cognos Series 7 provider will automatically use this configuration.

By configuring single signon, you are not prompted to reenter authentication information when accessing Cognos content that is secured by the Cognos Series 7 namespace.

Steps

1. Ensure that you configured Cognos 8 components to use a Cognos Series 7 namespace as an authentication provider (p. 263).
2. For Cognos Series 7, start Configuration Manager.
3. Click **Open the current configuration**.
4. On the **Components** tab, in the **Explorer** window, expand **Services**, **Access Manager - Runtime** and click **Cookie Settings**.
5. In the **Properties** window, ensure that the **Path**, **Domain**, and **Secure Flag Enabled** properties match the settings configured for Cognos 8.
6. Save and close Configuration Manager.
7. If the Cognos Series 7 namespace uses the Trusted Signon plug-in for single signon, you must now define the SaferAPIGetTrustedSignonWithEnv function.

You can now add Cognos Upfront Series 7 NewsBoxes to your Cognos Connection portal pages.

Cognos Series 7 Namespaces and the Cognos Series 7 Trusted Signon Plug-in

If the Cognos Series 7 namespace uses the Trusted Signon plug-in for single signon, you must define the SaferAPIGetTrustedSignonWithEnv function in your plug-in. Then you must recompile and redeploy the library for single signon to be achieved between Cognos 8 components and your authentication mechanism.

The SaferAPIGetTrustedSignonWithEnv function is an updated version of the SaferAPIGetTrustedSignon function. This update is required because Cognos 8 logon is not performed at the Web server as is the case for Cognos Series 7 applications. Therefore, it is not possible for the plug-in to perform a getenv() API call to retrieve Web server environment variables. The plug-in can request that specific environment variables be removed from the Web server using the SaferAPIGetTrustedSignonWithEnv function.

If you are running both Cognos Series 7 and Cognos 8 products using the same plug-in, both the SaferAPIGetTrustedSignonWithEnv and SaferAPIGetTrustedSignon functions are required. For information about the SaferAPIGetTrustedSignon function, see the Cognos Series 7 documentation.

SaferAPIGetTrustedSignonWithEnv Function

For users to be successfully authenticated by Access Manager, OS signons must exist and be enabled in the current namespace.

The memory for the returned trustedSignonName and trustedDomainName is allocated internally in this API. If the function returns SAFER_SUCCESS, Access Manager calls SaferAPIFreeTrustedSignon to free the memory allocated.

The memory for the returned reqEnvVarList is allocated internally in this API. If the function returns SAFER_INFO_REQUIRED, Access Manager calls SaferAPIFreeBuffer() to free the memory allocated.

Both functions, SaferAPIGetTrustedSignon and SaferAPIFreeBuffer must be implemented to successfully register the library when SaferAPIGetTrustedSignonWithEnv is implemented. The function SaferAPIGetError is required only if you want specific error messages returned from your plug-in.

Syntax

SaferAPIGetTrustedSignonWithEnv(

EnvVar	envVar[],	/*[IN]*/
char	**reqEnvVarList,	/*[OUT]*/
void	**trustedSignonName,	/*[OUT]*/
unsigned long	*trustedSignonNameLength,	/*[OUT]*/
void	**trustedDomainName,	/*[OUT]*/
unsigned long	*trustedDomainNameLength,	/*[OUT]*/
SAFER_USER_TYPE	*userType,	/*[OUT]*/
void	**implementerData);	/*[IN/OUT]*/

Parameter	Description
[in] envVar	An array of environment variable names and values that were retrieved from the Web server. The end of the array is represented by an entry with a null envVarName and a null envVarValue. Note that the first time this API is called, the envVar array contains only the end of array marker.
[in] reqEnvVarList	A string that contains a comma separated list of environment variable names that are requested by the Safer implementation. The end of the list must be null-terminated.

Parameter	Description
[out] trustedSignonName	A sequence of bytes that identifies the currently authenticated user. This value does not need to be null-terminated. This value is mandatory.
[out] trustedSignonNameLength	An integer value that indicates the length of the trustedSignonName. This length should exclude the null terminator, if there is one. This value is mandatory.
[out] trustedDomainName	A sequence of bytes that identifies the domain of the currently authenticated user. This value does not need to be null-terminated. If there is no trustedDomainName, the return is null. This value is optional.
[out] trustedDomainNameLength	An integer value that indicates the length of the trustedDomainName. This length should exclude the null terminator, if there is one. This value is mandatory and must be set to zero if there is no trustedDomainName.
[out] userType	A value that indicates the type of user that Access Manager will authenticate. This value is mandatory. The following return values are required for users to be successfully authenticated by Access Manager: SAFER_NORMAL_USER A named user. OS signons must exist and be enabled in the current namespace. SAFER_GUEST_USER A guest user. A guest user account must exist and be enabled in the current namespace. SAFER_ANONYMOUS_USER An anonymous user. An anonymous user account must exist and be enabled in the current namespace.
[in/out] implementerData	A pointer used to preserve implementation-specific data between invocations. An invocation occurs every time Access Manager calls the trusted signon plug-in. This value is valid only if the trusted signon plug-in was invoked and you set a value for it.

Configuring Cognos 8 to Use a Custom Authentication Provider

If you implemented a custom Java authentication provider with your existing security infrastructure, you can configure Cognos 8 components to use it.

You can use a custom authentication provider to access and authenticate users to an alternate authentication source. You can also use it as a single signon mechanism to integrate Cognos 8 components with your security infrastructure.

For more information, see the Custom Authentication Provider *Developer Guide*.

Configure a Custom Authentication Namespace

You can configure Cognos 8 components to use a custom authentication namespace. Any additional configuration for authentication source access, single signon, or custom attributes are dependent on the custom authentication provider implementation.

Steps

1. On every computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and click **New resource**, **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **Custom Java Provider** and then click **OK**.

   The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.
5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that Cognos 8 can locate and use your existing authentication provider.
7. From the **File** menu, click **Save**.
8. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

Cognos 8 loads, initializes, and configures the provider libraries for the namespace.

Configuring Cognos 8 Components to Use LDAP

You can configure Cognos 8 components to use an LDAP namespace as the authentication provider.

To bind a user to the LDAP server, the LDAP authentication provider must construct the distinguished name (DN). If the Use external identity property is set to True, it uses the External

identity mapping property to try to resolve the user's DN. If it cannot find the environment variable or the DN in the LDAP server, it attempts to use the User lookup property to construct the DN.

If users are stored hierarchically within the directory server, you can configure the User lookup and External identity mapping properties to use search filters. When the LDAP authentication provider performs these searches, it uses the filters you specify for the User lookup and External identity mapping properties. It also binds to the directory server using the value you specify for the Bind user DN and password property or using anonymous if no value is specified.

When an LDAP namespace has been configured to use the External identity mapping property for authentication, the LDAP provider binds to the directory server using the Bind user DN and password or using anonymous if no value is specified. All users who log on to Cognos 8 using external identity mapping see the same users, groups, and folders as the Bind user.

If you do not use external identity mapping, you can specify whether to use bind credentials to search the LDAP directory server by configuring the **Use bind credentials for search** property. When the property is enabled, searches are performed using the bind user credentials or using anonymous if no value is specified. When the property is disabled, which is the default setting, searches are performed using the credentials of the logged-on user. The benefit of using bind credentials is that instead of changing administrative rights for multiple users, you can change the administrative rights for the bind user only.

Important: If you use a DN syntax, such as *uid*=${*userID*}, ou=*mycompany*.com, for the properties **User lookup**, **External identity mapping**, or **Bind user DN and password,** you must escape all special characters that are used in the DN. If you use a search syntax, such as (*uid*=${*userID*}), for the properties **User lookup** or **External identity mapping**, you must not escape special characters that are used in the DN.

You also have the option of making custom user properties from the LDAP namespace available to Cognos 8 components.

To use an LDAP namespace and set up single signon, do the following:

- ❑ Configure Cognos 8 components to use an LDAP namespace
- ❑ Make custom user properties available to Cognos 8 components, if required
- ❑ Enable secure communication to the LDAP server, if required
- ❑ Enable single signon between LDAP and Cognos 8 components, if required

Configure an LDAP Namespace

You can configure Cognos 8 components to use an LDAP namespace when the users are stored in an LDAP user directory. The LDAP user directory may be accessed from within another server environment, such as Active Directory Server or eTrust SiteMinder.

If you are configuring an LDAP namespace for a directory server other than LDAP, see the appropriate section:

- For Active Directory Server, see Configure an LDAP Namespace for Active Directory Server.
- For IBM Directory Server, see Configure an LDAP Namespace for IBM Directory Server.

- For Novell Directory Server, see Configure an LDAP Namespace for Novell Directory Server.
- For Sun Java System Directory Server, see Configure an LDAP Namespace for Sun Java System Directory Server

Steps

1. On every computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and then click **New resource**, **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the appropriate namespace and then click **OK**.

   The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.
5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.
6. Specify the values for all other required properties to ensure that Cognos 8 components can locate and use your existing authentication provider.
7. If you want the LDAP authentication provider to bind to the directory server using a specific **Bind user DN and password** when performing searches, then specify these values.

   If no values are specified, the LDAP authentication provider binds as anonymous.

   If external identity mapping is enabled, **Bind user DN and password** are used for all LDAP access. If external identity mapping is not enabled, **Bind user DN and password** are used only when a search filter is specified for the **User lookup** property. In that case, when the user DN is established, subsequent requests to the LDAP server are executed under the authentication context of the end user.
8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following:
   - Ensure that **Use external identity** is set to **False**.
   - Set **Use bind credentials for search** to **True**.
   - Specify the user ID and password for **Bind user DN and password**.

   If you do not specify a user ID and password, and anonymous access is enabled, the search is done using anonymous.
9. Check the mapping settings for required objects and attributes.

   Depending on the LDAP configuration, you may have to change some default values to ensure successful communication between Cognos 8 components and the LDAP server.

LDAP attributes that are mapped to the **Name** property in **Folder mappings**, **Group mappings**, and **Account mappings** must be accessible to all authenticated users. In addition, the **Name** property must not be blank.

10. From the **File** menu, click **Save**.
11. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

Cognos 8 loads, initializes, and configures the provider libraries for the namespace.

Configure an LDAP Namespace for Active Directory Server

If you configure a new LDAP namespace for use with an Active Directory Server, you must modify the necessary settings and change the values for all properties of the Active Directory objects.

Steps

1. On every computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and then click **New resource**, **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the appropriate namespace and then click **OK**.

   The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.
5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that Cognos 8 components can locate and use your existing authentication provider.

   The following settings are examples:

   - For **User lookup**, specify (**sAMAccountName=${userID}**)
   - If you use single signon, for **Use external identity**, set the value to **True**.
   - If you use single signon, for **External identity mapping**, specify (**sAMAccountName=${environment("REMOTE_USER")}**)

     If you want to remove the domain name from the REMOTE_USER variable, specify (**sAMAccountName=${replace(${environment("REMOTE_USER")}, "*domain*\\","")}**).
   - For **Bind user DN and password**, specify ***user@domain***
   - For **Unique identifier**, specify **objectGUID**

7. If you want the LDAP authentication provider to bind to the directory server using a specific **Bind user DN and password** when performing searches, then specify these values.

   If no values are specified, the LDAP authentication provider binds as anonymous.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following:

   - Ensure that **Use external identity** is set to **False**.
   - Set **Use bind credentials for search** to **True**.
   - Specify the user ID and password for **Bind user DN and password**.

9. To configure the LDAP advanced mapping properties for use with the Active Directory Server objects, use the values specified in the following table.

   LDAP attributes that are mapped to the **Name** property in **Folder mappings**, **Group mappings**, and **Account mappings** must be accessible to all authenticated users. In addition, the **Name** property must not be blank.

Mappings	LDAP property	LDAP value
Folder	Object class	organizationalUnit,organization,container
	Description	description
	Name	ou,o,cn
Group	Object class	group
	Description	description
	Member	member
	Name	cn
Account	Object class	user
	Business phone	telephonenumber
	Content locale	(leave blank)
	Description	description
	Email	mail
	Fax/Phone	facsimiletelephonenumber

Mappings	LDAP property	LDAP value
	Given name	givenname
	Home phone	homephone
	Mobile phone	mobile
	Name	displayName
	Pager phone	pager
	Password	unicodePwd
	Postal address	postaladdress
	Product locale	(leave blank)
	Surname	sn
	Username	sAMAccountName

These mapping properties represent changes based on a default Active Directory Server installation. If you have modified the schema, you may have to make additional mapping changes.

10. From the **File** menu, click **Save**.
11. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

Cognos 8 loads, initializes, and configures the provider libraries for the namespace.

Configure an LDAP Namespace for IBM Directory Server

If you configure a new LDAP namespace for use with an IBM Directory Server, you must modify the necessary settings and change the values for all properties of the IBM Directory objects.

Steps

1. On every computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and then click **New resource**, **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **LDAP** and then click **OK**.

The new authentication namespace resource appears in the **Explorer** window, under the **Authentication** component.

5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.

6. Specify the values for all other required properties to ensure that Cognos 8 can locate and use your existing authentication namespace.
   - For **User lookup**, specify (**cn=${userID}**)
   - For **Bind user DN and password**, specify ***cn=root***

7. If you want the LDAP authentication provider to bind to the directory server using a specific **Bind user DN and password** when performing searches, then specify these values.

   If no values are specified, the LDAP authentication namespace binds as anonymous.

8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following:
   - Ensure that **Use external identity** is set to **False**.
   - Set **Use bind credentials for search** to **True**.
   - Specify the user ID and password for **Bind user DN and password**.

9. To configure the LDAP advanced mapping properties for use with IBM Directory Server objects, use the values specified in the following table.

   LDAP attributes that are mapped to the **Name** property in **Folder mappings**, **Group mappings**, and **Account mappings** must be accessible to all authenticated users. In addition, the **Name** property must not be blank.

Mappings	LDAP property	LDAP value
Folder	Object class	organizationalunit,organization,container
	Description	description
	Name	ou,o,cn
Group	Object class	groupofnames
	Description	description
	Member	member
	Name	cn

Mappings	LDAP property	LDAP value
Account	Object class	inetorgperson
	Business phone	telephonenumber
	Content locale	(leave blank)
	Description	description
	Email	mail
	Fax/Phone	facsimiletelephonenumber
	Given name	givenname
	Home phone	homephone
	Mobile phone	mobile
	Name	cn
	Pager phone	pager
	Password	userPassword
	Postal address	postaladdress
	Product locale	(leave blank)
	Surname	sn
	Username	uid

These mapping properties represent changes based on a default IBM Directory Server installation. If you have modified the schema, you may have to make additional mapping changes.

10. From the **File** menu, click **Save**.

Configure an LDAP Namespace for Novell Directory Server

If you configure a new LDAP namespace for use with a Novell Directory Server, you must modify the necessary settings and change the values for all properties of the Novell Directory objects.

Steps

1. On every computer where you installed Content Manager, open Cognos Configuration.

2. In the **Explorer** window, under **Security,** right-click **Authentication,** and then click **New resource, Namespace.**
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **LDAP** and then click **OK.**

   The new authentication namespace resource appears in the **Explorer** window, under the **Authentication** component.
5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that Cognos 8 can locate and use your existing authentication namespace.
   - For **User lookup**, specify (**cn=${userID}**)
   - For **Bind user DN and password,** specify the base DN for an administration user, such as **cn=*Admin*,0=*COGNOS***
7. If you want the LDAP authentication provider to bind to the directory server using a specific **Bind user DN and password** when performing searches, then specify these values.

   If no values are specified, the LDAP authentication namespace binds as anonymous.
8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following:
   - Ensure that **Use external identity** is set to **False.**
   - Set **Use bind credentials for search** to **True.**
   - Specify the user ID and password for **Bind user DN and password.**
9. To configure the LDAP advanced mapping properties for use with Novell Directory Server objects, use the values specified in the following table.

   LDAP attributes that are mapped to the **Name** property in **Folder mappings, Group mappings,** and **Account mappings** must be accessible to all authenticated users. In addition, the **Name** property must not be blank.

   For users to successfully log in to Cognos Connection, they must have permission to read the ou and o attributes.

Mappings	LDAP property	LDAP value
Folder	Object class	organizationalunit,organization,container
	Description	description
	Name	ou,o,cn

Mappings	LDAP property	LDAP value
Group	Object class	groupofnames
	Description	description
	Member	member
	Name	cn
Account	Object class	inetOrgPerson
	Business phone	telephonenumber
	Content locale	Language
	Description	description
	Email	mail
	Fax/Phone	facsimiletelephonenumber
	Given name	givenname
	Home phone	homephone
	Mobile phone	mobile
	Name	cn
	Pager phone	pager
	Password	(leave blank)
	Postal address	postaladdress
	Product locale	Language
	Surname	sn
	Username	uid

These mapping properties represent changes based on a default Novell Directory Server installation. If you have modified the schema, you may have to make additional mapping changes.

10. From the **File** menu, click **Save**.

Configure an LDAP Namespace for Sun Java System Directory Server

If you configure a new LDAP namespace for use with Sun Java System Directory Server, you must modify the necessary settings and change the values for all properties of the Sun Java System Directory objects.

Steps

1. On every computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and then click **New resource**, **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **LDAP** and then click **OK**.

   The new authentication namespace resource appears in the **Explorer** window, under the **Authentication** component.
5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that Cognos 8 can locate and use your existing authentication namespace.

   The following settings are examples:

   - For **User lookup**, type (**uid=${userID}**)
   - If you use single signon, for **Use external identity**, set the value to **True**.
   - If you use single signon, for **External identity mapping**, specify any attribute, such as the NT user domain ID or the user ID:

     (**ntuserdomainid=$environment("REMOTE_USER")**})

     (**uid=${environment("REMOTE_USER")**})
   - For **Unique identifier**, type **nsuniqueid**
7. If you want the LDAP authentication provider to bind to the directory server using a specific **Bind user DN and password** when performing searches, then specify these values.

   If no values are specified, the LDAP authentication namespace binds as anonymous.
8. If you do not use external identity mapping, use bind credentials for searching the LDAP directory server by doing the following:

   - Ensure that **Use external identity** is set to **False**.
   - Set **Use bind credentials for search** to **True**.

- Specify the user ID and password for **Bind user DN and password**.

9. To configure the LDAP advanced mapping properties for use with Sun Java System Directory Server objects, use the values specified in the following table.

   LDAP attributes that are mapped to the **Name** property in **Folder mappings**, **Group mappings**, and **Account mappings** must be accessible to all authenticated users. In addition, the **Name** property must not be blank.

Mappings	LDAP property	LDAP value
Folder	Object class	organizationalUnit,organization
	Description	description
	Name	ou,o
Group	Object class	groupofuniquenames
	Description	description
	Member	uniquemember
	Name	cn
Account	Object class	inetorgperson
	Business phone	telephonenumber
	Content locale	preferredlanguage
	Description	description
	Email	mail
	Fax/Phone	facsimiletelephonenumber
	Given name	givenname
	Home phone	homephone
	Mobile phone	mobile
	Name	cn
	Pager phone	pager

Mappings	LDAP property	LDAP value
	Password	userPassword
	Postal address	postaladdress
	Product locale	preferredlanguage
	Surname	sn
	Username	uid

These mapping properties represent changes based on a default Sun Java System Directory Server installation. If you have modified the schema, you may have to make additional mapping changes.

10. From the **File** menu, click **Save**.

Make Custom User Properties for LDAP Available to Cognos 8 Components

You can use arbitrary user attributes from your LDAP authentication provider in Cognos 8 components. To configure this, you must add these attributes as custom properties for the LDAP namespace. The custom properties are available as session parameters through Framework Manager. For more information about session parameters, see the Framework Manager *User Guide*.

The custom properties can also be used inside command blocks that are used to configure Oracle sessions and connections. The command blocks can be used with Oracle lightweight connections and virtual private databases. For more information, see the *Administration and Security Guide*.

Steps

1. On every computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security**, **Authentication**, click the LDAP namespace.
3. In the **Properties** window, click in the **Value** column for **Custom properties** and click the edit button.
4. In the **Value - Custom properties** window, click **Add**.
5. Click the **Name** column, and enter the name you want Cognos 8 components to use for the session parameter.
6. Click the **Value** column, and enter the name of the account parameter in your LDAP authentication provider.
7. Repeat the preceding two bulleted steps for each custom parameter.
8. Click **OK**.

9. From the **File** menu, click **Save**.

Enable Secure Communication to the LDAP Server

Secure LDAP protocol (LDAPS) encrypts the communication between the Access Manager component of Content Manager and the directory server. LDAPS prevents sensitive information in the directory server and the LDAP credentials from being sent as clear text.

To enable LDAPS, install a server certificate that is signed by a certificate authority in the directory server. Next, create a certificate database to contain the certificates. Finally, configure the directory server and the Cognos 8 LDAP namespace to use LDAPS.

The server certificate must be a copy of either

- the trusted root certificate and all other certificates that make up the chain of trust for the directory server certificate

  The trusted root certificate is the certificate of the root certificate authority that signed the directory server certificate.

- the directory server certificate only

The certificates must be Base64 encoded in ASCII (PEM) format. All certificates except the trusted root certificate must not be self-signed.

You must use the certutil tool from Netscape OpenSource toolkit NSS_3_3_2_RTM to create the certificate database. Cognos 8 does not accept other versions of cert7.db files, including those from the certutil tool that is provided with Microsoft Active Directory. The appropriate certutil tool is available from ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_3_2_RTM.

For UNIX and Linux, you must also use the NSPR library, which is available from ftp://ftp.mozilla.org/pub/mozilla.org/nspr/releases/v4.1.2.

Steps

1. Create a directory for the certificate database.
2. Create the certificate database by typing

   certutil -N -d *certificate_directory*

   where *certificate_directory* is the directory that you created in step 1.

   This command creates a cert7.db file and a key3.db file in the new directory.
3. Add the certificate authority (CA) certificate or the directory server certificate to the certificate database by typing the appropriate command for the type of certificate:
   - For a CA certificate, type

     certutil -A -n *certificate_name* -d *certificate_directory* -i CA.cert -t C,C,C

   - For a directory server certificate, type

     certutil -A -n *certificate_name* -d *certificate_directory* -i *server_certificate*.cert -t P

where *certificate_name* is an alias that you assign, such as the CA name or host name; and *server_certificate* is the prefix of the directory server certificate file.

4. Copy the certificate database directory to the *c8_location*/configuration directory on every computer where Content Manager is installed.
5. Configure the directory server to use LDAPS and restart the directory server.

   For more information, see the documentation for the directory server.
6. On the Content Manager computer where you configured the LDAP namespace to use the directory server, start Cognos Configuration.
7. In the **Explorer** window, under **Security**, **Authentication**, click the LDAP namespace.
8. In the **Properties** window, for the **Host and port** property, change the port to the secure LDAPS port.

   For the **SSL certificate database** property, specify the path to the cert7.db file.
9. In the **Explorer** window, right-click the LDAP namespace and click **Test**.

   If the test fails, revise the properties, ensuring that the correct certificate is used.
10. From the **File** menu, click **Save**.
11. From the **Actions** menu, click **Restart**.
12. Repeat steps 6 to 11 on every other computer where Content Manager is installed.

Enabling Single Signon Between LDAP and Cognos 8 Components

You achieve single signon to Cognos 8 components by configuring the External Identity mapping property.

The External Identity mapping can refer to a CGI environment variable or an HTTP header variable. In the case of an application server gateway or dispatcher entry pointing to Cognos 8 components, the External Identity mapping can refer to the userPrincipalName session variable. The resolved value of the External Identity mapping property at runtime must be a valid user DN.

When an LDAP namespace is configured to use the External Identity mapping property for authentication, the LDAP provider binds to the directory server using the Bind user DN and password or using anonymous if no value is specified. All users who log on to Cognos 8 using external identity mapping see the same users, groups, and folders as the Bind user.

If you want Cognos 8 components to work with applications that use Java or application server security, you can configure the External identity mapping property to obtain the user ID from the Java user principal. Include the token ${environment("USER_PRINCIPAL")} in the value for the property. For more information, see the online help for Cognos Configuration.

You can apply limited expression editing to the External Identity mapping property using the replace operation.

Replace Operation

The replace operation returns a copy of the string with all occurrences of the old substring replaced by the new substring.

The following rules apply:

- The character \ is used to escape the characters in the function parameters. Characters such as \ and " need escaping.
- Nested function calls are not supported.
- Special characters are not supported.

Syntax

${replace(str , old , new)}

Parameter	Description
str	The string to search.
old	The substring to be replaced by the new substring.
new	The substring that replaces the old substring.

Examples

${replace(${environment("REMOTE_USER")},"NAMERICA\\",)}

${replace(${environment("REMOTE_USER")},"NAMERICA\\","")}

Configuring Cognos 8 Components to Use eTrust SiteMinder

You can configure Cognos 8 components to use a Netegrity SiteMinder namespace as the authentication source, provided that you installed Content Manager on a non-Linux computer.

To configure an authentication provider in an eTrust SiteMinder environment, you configure an LDAP, NTLM, or Netegrity SiteMinder namespace depending on your eTrust SiteMinder configuration. Supported eTrust SiteMinder configurations are LDAP, Active Directory Server, and NTLM user directories.

Note: The authentication provider uses an eTrust SiteMinder SDK to implement a custom agent, and the custom agent deployment requires that the Agent Properties in the eTrust SiteMinder Policy server administration console be set to be able to support 4.x agents.

If eTrust SiteMinder is Configured For More Than One User Directory

If you configured eTrust SiteMinder for more than one user directory, you must use the Netegrity SiteMinder namespace. After configuring the Netegrity SiteMinder namespace in Cognos 8, you

must also add a corresponding LDAP, Active Directory Server, or NTLM namespace to the Cognos configuration for each user directory defined in eTrust SiteMinder.

When configuring a corresponding LDAP namespace, you must ensure that the External identity mapping property is enabled and that you include the token REMOTE_USER in the value for the property. This does not mean that eTrust SiteMinder must be configured to set REMOTE_USER. The Cognos Netegrity SiteMinder namespace passes user information internally to the corresponding LDAP namespace when it receives successful user identification from the eTrust SiteMinder environment.

When configuring a corresponding Active Directory namespace, you must ensure that the singleSignOnOption property is set to IdentityMapping. The Cognos Netegrity SiteMinder namespace passes user information internally to the corresponding LDAP namespace using the REMOTE_USER environment variable when it receives successful user identification from the eTrust SiteMinder environment. For more information, see "Enabling Single Signon Between Active Directory Server and Cognos 8 Components" (p. 262).

If eTrust SiteMinder is Configured With Only One User Directory

If eTrust SiteMinder is configured with only one user directory, the Netegrity SiteMinder namespace is not required. You can use the user directory as your authentication source by configuring the appropriate namespace, or you can configure the eTrust SiteMinder provider with one user directory. For example, if the eTrust SiteMinder user directory is NTML, you can configure Cognos 8 components with an NTLM namespace or configure Cognos 8 components with one Netegrity SiteMinder namespace, referring to one user directory that is an NTLM namespace.

If the eTrust SiteMinder user directory is Active Directory, you can use an Active Directory namespace or an LDAP namespace that is configured for use with Active Directory.

If you want to use the user directory as your authentication source directly instead of configuring a Netegrity SiteMinder namespace, configure the appropriate LDAP (p. 269), Active Directory (p. 271), or NTLM (p. 286) namespace. In this case, you must verify the Agent Configuration Object properties in eTrust SiteMinder Policy Server. Ensure that SetRemoteUser is activated.

When configuring the LDAP namespace, in this case, you must ensure that the External identity mapping property is enabled and that you include the token REMOTE_USER in the value for the property.

When configuring the Active Directory namespace, in this case, you must ensure that the singleSignOnOption property is set to IdentityMapping. For more information, see "Enabling Single Signon Between Active Directory Server and Cognos 8 Components" (p. 262).

To use an eTrust SiteMinder namespace and to set up single signon, do the following:

- Configure Cognos 8 components to use a Netegrity SiteMinder namespace
- Enable secure communication to the eTrust SiteMinder user directory, if required
- Enable single signon between eTrust SiteMinder and Cognos 8
- Protect the Cognos Web alias.

Configure a Netegrity SiteMinder Namespace

If you configured eTrust SiteMinder for more than one user directory, you must use the Netegrity SiteMinder namespace. After adding the Netegrity SiteMinder namespace, you must also add a corresponding LDAP or NTLM namespace for each user directory.

You can also configure an Netegrity SiteMinder namespace if users are stored in

- an LDAP server
- an NTLM server
- an Active Directory server

Steps

1. On the computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and click **New resource**, **Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click the Netegrity SiteMinder namespace and then click **OK**.

   The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.
5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all other required properties to ensure that Cognos 8 components can locate and use your existing authentication provider.
7. In the **Explorer** window, under **Security**, **Authentication**, right-click the namespace and click **New resource**, **SiteMinder Policy Server**.
8. In the **Name** box, type a name for the policy server and click **OK**.
9. In the **Properties** window, specify the **Host** property and any other property values you want to change.
10. In the **Explorer** window, right-click the new SiteMinder Policy Server and click **New resource**, **User directory**.

    Tip: Configure a user directory for each user directory in the SiteMinder policy server.
11. In the **Name** box, type a name for the user directory and click **OK**.

    Important: The name of the user directory must match the name that appears on the policy server.
12. In the **Properties** window, type a value for the **Namespace ID reference** property.

13. From the **File** menu, click **Save**.
14. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.
15. Configure a corresponding LDAP, Active Directory, or NTLM namespace for each LDAP, Active Directory, or NTLM user directory.

    Important: Ensure that you use the same value for the **Namespace ID** property that you use for the **Namespace ID** property for the Netegrity SiteMinder namespace.

Enabling Secure Communication to the eTrust SiteMinder User Directory

If you use an SSL connection to the directory server, you must appropriately configure the Cognos namespace for the user directory.

For more information, see "Configure an LDAP Namespace" (p. 269).

Enable Single Signon Between eTrust SiteMinder and Cognos 8

By configuring single signon, you are not prompted to reenter authentication information.

Cognos 8 components automatically refer to the eTrust SiteMinder session cookie for user session data.

If the eTrust SiteMinder user directory is LDAP or Active Directory, you must configure the eTrust SiteMinder user directory to use external identity mapping to the REMOTE_USER environment variable.

If the eTrust SiteMinder user directory is NTLM, Integrated Windows Authentication is used for single signon and no additional configuration is required.

Protecting the Cognos Web Alias

eTrust SiteMinder must be configured correctly to protect the Cognos Web alias.

Use the test tool provided with eTrust SiteMinder to verify that the resource is protected, authenticated, and authorized. For more information, see your eTrust SiteMinder documentation.

Configuring Cognos 8 Components to Use an NTLM Namespace

You can configure Cognos 8 components to use the Windows native security, NT LAN Manager (NTLM), as the authentication source.

If you are not using NTLM in your IS environment, you cannot use an NTLM namespace.

If you want to use an NTLM user directory as your authentication source with eTrust SiteMinder, you must verify the Agent Configuration Object properties in the eTrust SiteMinder Policy Server. Ensure that SetRemoteUser is activated.

To use NTLM and to set up single signon, do the following:

- configure an NTLM namespace
- enable single signon between NTLM and Cognos 8 components

Configure an NTLM Namespace

You can configure Cognos 8 components to use an NTLM namespace when users are stored in an NTLM user directory. The NTLM user directory may also be accessed using an eTrust SiteMinder authentication provider.

Steps

1. On the computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security,** right-click **Authentication**, and click **New resource, Namespace**.
3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **NTLM** and click **OK**.

   The new authentication provider resource appears in the **Explorer** window, under the **Authentication** component.
5. In the **Properties** window, for the **NamespaceID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the **NamespaceID** property.
6. Specify the values for all other required properties to ensure that Cognos 8 components can locate and use your existing authentication provider.
7. From the **File** menu, click **Save**.
8. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

Cognos 8 loads, initializes, and configures the provider libraries for the namespace.

Enable Single Signon Between NTLM and Cognos 8 Components

By default, the Cognos NTLM provider integrates with the IIS Web server for single signon if Windows integrated authentication (formerly named NT Challenge Response) is enabled on the IIS Web server.

If Windows integrated authentication is enabled, you are not prompted to reenter authentication information when accessing Cognos content that is secured by the NTLM namespace.

Steps

1. Set up Windows integrated authentication on the IIS Web server.

2. Install Content Manager on a computer that is part of the domain, for the active and standby Content Manager computers.
3. Set up the computers, or the user account under which Content Manager runs, to be trusted for delegation.
4. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

Cognos 8 loads, initializes, and configures the provider libraries for the namespace.

Configuring Cognos 8 to Use SAP

To use an SAP server as your authentication provider, you must use a supported version of SAP BW. To review an up-to-date list of environments supported by Cognos products, such as operating systems, patches, browsers, Web servers, directory servers, database servers, and application servers, visit the Cognos Global Customer Services Web site (http://support.cognos.com). In addition, Content Manager must be installed on a non-Linux computer.

In SAP BW, you can assign users to user groups or roles or both. The SAP authentication provider uses only the roles.

The authorization rights required by the SAP user depend on who uses Cognos 8 components, users or administrators.

SAP Authorization Settings for Cognos 8 Users

The following authorization objects are required for any Cognos user. Some of the values shown, such as *, are default values that you may want to modify for your environment.

Authorization object	Field	Value
S_RFC Authorization check for RFC access	Activity	
	Name of RFC to be protected	RFC1 RS_UNIFICATION, SDTX, SH3A, SU_USER, SYST, SUSO
	Type of RFC to be protected	FUGR
S_USER_GRP User Master Maintenance: User Groups	Activity	03
	Name of user group	*

SAP Authorization Settings for Cognos Administrators

If users will perform administrative tasks and searches for users and roles, the following values must be added to the S_RFC authorization object in addition to the values listed above for Cognos 8 users. Some of the values shown, such as *, are default values that you may want to modify for your environment.

Authorization object	Field	Value
S_RFC Authorization check for RFC access	Activity	16
	RFC_NAME	PRGN_J2EE, SHSS, SOA3
	Type of RFC object to be protected	FUGR

Connectivity Between SAP BW and Cognos 8 on UNIX

To configure connectivity between SAP BW and Cognos 8 components on a UNIX operating system, ensure that you install the SAP shared library file (provided by SAP) and add it to the library path environment variable as follows:

- Solaris

  LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<librfccm.so_directory>

- HP-UX

  SHLIB_PATH=$SHLIB_PATH:<librfccm.sl_directory>

- AIX

  LIBPATH=$LIBPATH:<librfc.a_directory>

To use SAP and to set up single signon, do the following:

- ❑ Configure Cognos 8 components to use an SAP namespace
- ❑ Enable single signon between SAP and Cognos 8 components

Configure an SAP Namespace

You can configure Cognos 8 components to use an SAP server as the authentication source.

Steps

1. On the computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication**, and click **New resource**, **Namespace**.

3. In the **Name** box, type a name for your authentication namespace.
4. In the **Type** list, click **SAP** and then click **OK**.

   The new authentication provider resource appears in the **Explorer** window, under the Authentication component.
5. In the **Properties** window, for the **Namespace ID** property, specify a unique identifier for the namespace.

   Tip: Do not use colons (:) in the Namespace ID property.
6. Specify the values for all required properties to ensure that Cognos 8 components can locate and use your existing authentication provider.

   Depending on your environment, for the **Host** property, you may have to add the SAP router string to the SAP host name.
7. If the SAP system encodes the contents of cookies, enable the decode tickets feature:
   - In the **Properties** window, for **Advanced properties**, click the Value and then click the edit button.
   - Click **Add**.
   - Enter the name **URLDecodeTickets** and enter the value **true**
   - Click **OK**.

   All SAP logon tickets will be decoded by the SAP namespace before establishing a connection.
8. From the **File** menu, click **Save**.
9. Test the connection to a new namespace. In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

Enable Single Signon Between SAP and Cognos 8

You can enable single signon between SAP Enterprise Portal and Cognos 8 components as well as when using the external namespace function of the SAP BW data source connections. To do so, ensure that you set the following system parameters on the SAP BW server:

- login/accept_sso2_ticket = 1
- login/create_sso2_ticket = 1
- login/ticket_expiration_time = 200

Test the Namespaces

After you configure one or more new namespaces for Cognos 8 components, you can test the namespaces. The test can occur before or after you start the Cognos 8 service. You can test all namespaces at the same time or test them individually.

Step to Test All Namespaces

- In the **Explorer** window, right-click **Authentication** and click **Test**.

  Cognos 8 components load, initialize, and configure the provider libraries for one namespace before testing the next namespace.

  Tip: To cancel a namespace test, click **Cancel**. The test stops when the current namespace test is complete.

Step for a Single Namespace

- In the **Explorer** window, under **Authentication**, right-click the new authentication resource and click **Test**.

  Cognos 8 components load, initialize, and configure the provider libraries for the namespace.

Delete an Authentication Provider

If they are no longer required, you can delete namespaces that you added or unconfigured namespaces that Cognos 8 components detected.

Important: You must not delete the Cognos namespace. It contains authentication data that pertains to all users and is required to save the configuration.

When you delete a namespace, you can no longer log on to the namespace. Security data for the namespace remains in Content Manager until you permanently delete it in the portal. For more information, see the *Administration and Security Guide*.

After you delete a namespace, it appears as Inactive in the portal.

Steps

1. On a computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security**, **Authentication**, right-click the namespace and click **Delete**.
3. Click **Yes** to confirm.

   The namespace disappears from the **Explorer** window and you can no longer log on to the namespace on that computer.
4. From the **File** menu, click **Save**.
5. Repeat steps 1 to 4 for each computer where you installed Content Manager.

You must now log on to the portal and permanently delete the data for the namespace. For more information, see the *Administration and Security Guide*.

Chapter 12: Configuring Cognos 8 for a Third-Party Application Server

Cognos 8 installs and uses Tomcat as the application server by default. You can choose to run Cognos 8 within one of the following supported third-party application servers instead:

- BEA WebLogic Server
- IBM WebSphere Application Server
- Oracle Application Server
- Red Hat JBoss
- SAP Web Application Server

To ensure your product works properly, apply all required operating system patches and use only the versions of third-party software that are supported for a Cognos product.

To review an up-to-date list of environments supported by Cognos products, such as operating systems, patches, browsers, Web servers, directory servers, database servers, and application servers:

- Visit the Cognos Global Customer Services Web site (http://support.cognos.com).

  It is important to note that the Linux operating system is available in a number of distributions and supports a number of hardware platforms. Ensure that the operating system and hardware combination you are using is a supported combination.

  When you install Cognos 8 on Linux, Framework Manager is not installed. The BMTScriptPlayer is a command-line utility that interfaces with the Framework Manager engine, allowing you to run Framework Manager action logs. Because Framework Manager is not installed, the BMTScriptPlayer will not work.

You can choose to run the Cognos Servlet Gateway on a supported application server instead of using a Web server (p. 233). When using the servlet gateway, your environment does not require a Web server. The application server and the servlet gateway replace the functions provided by the Web server and other Cognos gateways. Cognos 8 must be installed and running prior to configuring and deploying the Cognos Servlet Gateway.

If you are upgrading from ReportNet to Cognos 8, see "Upgrade to Cognos 8 in an Application Server Environment " (p. 311).

If you are upgrading from Metrics Manager to Cognos 8 Metrics Manager, see "Upgrade from Metrics Manager to Cognos 8 in an Application Server Environment" (p. 312).

For information about configuring a multi-server distributed installation of Cognos 8 in an application server environment, contact Cognos support (http://support.cognos.com).

To set up Cognos 8 to run on your application server, do the following:

- ❑ Create a separate JVM instance, if necessary.
- ❑ Check that Cognos components are properly set up.
- ❑ Back up any existing Cognos data and encryption keys, if required.
- ❑ Set environment variables.
- ❑ Update the Java environment.
- ❑ Configure Cognos components to run within the application server.
- ❑ Identifying the JDK for WebLogic 9 on AIX, if necessary.
- ❑ Change the application server startup script, if necessary.
- ❑ Change the Cognos dispatcher properties file, if using Oracle Application Server.
- ❑ Configure application server properties and deploy Cognos 8.
- ❑ Enable SSL, if required.
- ❑ Configure the web server.
- ❑ Unregister dispatchers that are no longer used.
- ❑ Import any backed up content store data.

After setting up Cognos 8 to run on your application server, you can perform some additional configuration tasks to customize the behavior of Cognos components to better suit your reporting environment (p. 193). You can also test your configuration (p. 192).

Tip: Do not use install paths that contain spaces for the application server or Cognos 8. Spaces interfere with the internal scripts and command parameters. If you must use an install path that includes spaces, use the 8.3 DOS naming convention when referring to these locations.

Create a Separate JVM Instance

To eliminate potential java class or system resource conflicts, Cognos 8 must be run in a Java Virtual Machine (JVM) instance isolated from other existing applications. This ensures that Cognos 8 does not affect any existing customer applications. When possible, Cognos 8 must be installed in a JVM instance that is separate from the application server admin processes to isolate both Cognos 8 and the administrative functions of the application server.

An isolated JVM instance can be established by creating one of the following:

- a separate managed server in BEA WebLogic
- a separate server instance in IBM WebSphere
- a separate OC4J instance in Oracle 10g Application Server
- a separate server instance for Red Hat JBoss
- a separate Java instance for SAP Web Application Server

If you are using the Cognos Servlet Gateway, it must be run in an instance that is separate from Cognos 8.

Check the Setup of Cognos Components

Ensure that the following is done before you set up Cognos components to run on the application server:

- Cognos components are installed (p. 93).
- Before you start Cognos 8, the database for the content store must be set up. Install and configure the database clients, if required (p. 159), and then test the database connectivity.
- The application server is installed and operational on each computer where Cognos components are installed.

  For more information about installation, see your application server documentation.
- The fully qualified installation location of all fonts is specified on all Application Tier Component computers. You specify this location in Cognos Configuration (p. 206). By default, the installation location does not use a fully qualified path.
- The application server user account has full access permissions for the Cognos installation.

  Tip: We recommend that you create a new UNIX or Linux group named cognos8. This group must contain the user that starts the application server and the user that owns the Cognos files. Change the group ownership of the Cognos files to the cognos8 group and change the file permissions for all Cognos files to GROUP READABLE/WRITABLE/EXECUTABLE. For simplicity, you can also use the application server user account to install and run Cognos components.

Back Up Existing Cognos Information

You must back up existing Cognos information if Cognos 8 components are running

- on an application server (including Tomcat) and you are changing to an application server that ships with its own JVM.
- with a JVM from one vendor and you are changing to another JVM vendor.

Note: You must back up existing Cognos information within the working environment prior to upgrade.

Before configuring Cognos 8 components to run on the new application server or JVM, you must back up

- content store data by creating a deployment export.
- configuration information by exporting it. Any encrypted data is decrypted during the export.

- cryptographic keys by saving them to an alternate location. New cryptographic keys must be created using the same JVM that the application server uses. Because these keys can be created only if the previous keys are deleted, it is important to back up the previous keys.

To ensure the security and integrity of your Cognos data, back up the content store, configuration information, and cryptographic keys to a directory that is protected from unauthorized or inappropriate access.

Tip: To check if any cryptographic keys exist, look in the *c8_location*/configuration directory. Cryptographic keys exist if this directory includes the following subdirectories: csk, encryptkeypair or signkeypair.

Steps

1. If data exists in the content store, start the Cognos 8 service and export the entire content store using the Deployment tool.

   For more information, see the topic about creating an export deployment specification in the *Administration and Security Guide*.

2. In Cognos Configuration, from the **File** menu, click **Export As** and save the configuration information in a decrypted format. When naming the file, use a name such as "decrypted.xml".

   Export the data to a directory that is protected from unauthorized or inappropriate access because passwords are stored in plain text. You are prompted to acknowledge that the export is an unsecure operation.

3. Stop the Cognos 8 service:
   - If you use Tomcat, stop the Cognos 8 service and close Cognos Configuration.
   - If you use an application server other than Tomcat, shut down Cognos 8 in your environment.

4. Back up any existing cryptographic keys by saving the appropriate files and directories to an alternate location that is secure.

   The files are
   - *c8_location*/configuration/cogstartup.xml
   - *c8_location*/configuration/caSerial
   - *c8_location*/configuration/cogconfig.prefs
   - *c8_location*/configuration/coglocale.xml

   The directories are
   - *c8_location*/configuration/csk
   - *c8_location*/configuration/encryptkeypair
   - *c8_location*/configuration/signkeypair

5. Delete the caSerial and cogconfig.prefs files and the three directories: csk, encryptkeypair, and signkeypair.

6. Replace the *c8_location*/configuration/cogstartup.xml file with the file that contains the data exported from Cognos Configuration (for example, "decrypted.xml").

   Important: In the *c8_location*/configuration directory, the file must use the name "cogstartup.xml".

   The information in this file will be automatically re-encrypted using new cryptographic keys when you save the configuration in Cognos Configuration.

Set Environment Variables

You must set environment variables to identify the location of the JVM environment and the library path. You can set environment variables using any of the following methods:

- On Windows, set a system or user variable, or edit the application server's startup environment script.

  If you set a user variable, ensure that you set it for the user account that will run the application server, or administration console.

- On UNIX and Linux, set an environment variable in the user profile, or edit the application server's startup or environment script.

For information about editing an application server's startup script, see "Change the Application Server Startup Script" (p. 301).

Tip: Most application server versions ship with a script specifically intended for setting environment variables. For example, some WebSphere versions ship with setupCmdLine.bat or setupCmdLine.sh, WebLogic ships with setEnv.cmd or setEnv.sh, and Oracle ships with iasenv.bat or iasenv.sh. These scripts can be modified to set appropriate values for use with Cognos components. Most of these scripts set the JAVA_HOME environment variable by default.

Steps

1. Set the JAVA_HOME environment variable to point to the JVM used by the application server.

   Tip: If the application server ships with a JVM, then the JAVA_HOME environment variable must be set to reference it.

   Cognos Configuration uses this variable to create encryption keys for Cognos components that are compatible with the JVM used by the application server.

   For example, for WebLogic under Windows, the JVM used by the application server is specified as:

   drive:/*WebLogic_location*/jdk142_04

2. Append *c8_location*/bin to the appropriate environment variable.

   This variable is used to locate the Cognos library files.

Operating system	Environment variable
Windows	PATH
AIX	LIBPATH
Solaris and Linux	LD_LIBRARY_PATH
HP-UX	SHLIB_PATH

Tip: To install multiple instances of Cognos 8 on a single server, set the PATH, LIBPATH, LD_LIBRARY_PATH, or SHLIB_PATH variable within the application server instance scope and not as a global variable to ensure that each instance has a unique value.

Note: The CRN_ROOT and COG_ROOT variables are no longer required in a non-clustered environment and should be removed if they were used in a previous installation.

Update the Java Environment

Cognos 8 cryptographic services use a specific .jar (Java Archive) file, named bcprov-jdk*nn-nnn*, that must be located in the JVM environment used by your application server. This file provides additional encryption and decryption routines that are not supplied with a default JVM installation. To ensure security, the encryption file must be loaded by the JVM using the Java extensions directory.

Steps

1. Ensure that the JAVA_HOME environment variable is set to the JRE location.

   For example, to set JAVA_HOME to the JRE files provided with the installation, the path is *c8_location*/bin/jre/*version*.

2. Copy the bcprov-jdk*nn-nnn*.jar file from the *c8_location*/bin/jre/*version*/lib/ext directory to the *Java_location*/jre/lib/ext directory.

Configure Cognos Components to Run Within the Application Server

Cognos 8 must be configured with the application server configuration information, and the configuration must be saved to create new cryptographic keys. Cognos Configuration uses the JVM that is defined by the JAVA_HOME environment variable.

Important: You must set the JAVA_HOME environment variable to the JVM supplied or used by the application server and then copy the security provider files before you run Cognos Configuration to ensure valid encryption keys are generated.

Steps

1. From the *c8_location*/bin directory, start Cognos Configuration:
   - On Windows, type **cogconfig.bat** in a command window or select **Cognos Configuration** from the **Start** menu.
   - On UNIX or Linux, type **cogconfig.sh**

   If you have existing incompatible encryption keys, you will be prompted to automatically generate new ones at this time.

   Tip: Ensure that the existing keys are backed up to a secure location before proceeding. There is no undo action available after you generate new keys.

2. Use the Build Application Wizard to create the application file that will be deployed to the application server. To launch the Build Application Wizard from Cognos Configuration under **Actions**, click **Build Application Files**. The wizard allows you to select the type of application to build and the context root used to access the application.

   You must build the application file on the same computer on which you will be deploying the file.

   The context root value entered in the wizard must be the same as is entered in the Environment tab, and used to deploy to the application server. For Cognos 8, the default context root and application directory name is p2pd, which can be used in most cases. For the Cognos Servlet Gateway, the default context root and application directory name is ServletGateway. Other default application deployment values, such as the application name, may be changed to better suit your environment.

   Tip: It is not necessary to rebuild or redeploy the archive file when you make configuration changes because configuration information is stored externally to the application.

   For WebLogic and JBoss, you can use the Build Application wizard in Cognos Configuration to build the application to an expanded directory.

   For example, for WebLogic, you put the application in C:\bea\user_projects\domains\apps\p2pd, where p2pd is the name of the application. When deploying the application from the WebLogic Administration Console, you would select the p2pd directory.

   Important: For JBoss, if you use the Expand files into a folder option, you must include the .war extension in the name of the folder where the wizard will create the p2pd application. When the wizard prompts for the folder location, go to *JBoss_location*/server/*instance_name*/deploy and create a folder named p2pd.war.

   For information about which type of application file, WAR, EAR or expanded directory, is supported in your environment, see your application server documentation.

3. In the **Explorer** window of Cognos Configuration, expand **Environment** and then change the following properties to use the port number and host name or IP address of the server where the Cognos 8 component and application server are installed.
   - All URIs for the dispatcher, including

     Dispatcher URIs for Gateway

     External dispatcher URI

     Internal dispatcher URI

     Dispatcher URI for external applications
   - **Gateway URI**
   - **Content Manager URIs**

   The application server must be configured to listen on the host name or IP address entered in the URI. For more information, see your application server documentation.

   If you change the context root from the default value of p2pd, you must change the context root portion of the URI as well.
4. Under **Environment**, **Cognos 8 service**, right-click **Cognos 8**, and then click **Delete**.

   The entry for the Cognos 8 service is used to configure environment settings for running under Tomcat. The entry is not required when using a different application server.
5. Complete other required configuration changes such as
   - specifying properties for the Content Manager database
   - entering user IDs and passwords

   If you used the default settings for the Cognos installation, you may only have to make minor changes to the default configuration settings (p. 193). You can review the configuration for single computer installations (p. 146) or for distributed installations (p. 156) to determine if there are any additional changes required.
6. Save the configuration.

   New cryptographic keys are created using the JVM that is defined by the JAVA_HOME variable.
7. Close Cognos Configuration.

Identifying the JDK for WebLogic 9 on AIX

WebLogic 9 requires JDK 1.5. If you use WebLogic Server 9 on AIX, you must update the Java options in the commEnv.sh file to specify the appropriate serial version unique identifier (UID). If

you do not make this update, a serial version UID mismatch occurs when using WebLogic Server 9 with IBM Java 5.

Steps

1. Open the *WebLogic9_location*/common/bin/commEnv.sh file.
2. Modify the file to include the following command:

```
JAVA_OPTIONS="${JAVA_OPTIONS}
-Dcom.sun.xml.namespace.QName.useCompatibleSerialVersionUID=1.0"
export JAVA_OPTIONS
```

3. Save and close the commEnv.sh file.

Change the Application Server Startup Script

Some application servers have specific requirements that you must meet before you can run Cognos 8. Depending on the application server, you may have to define environment variables, copy files, and add or change code in files.

If you are using BEA WebLogic Server 8.1 or Red Hat JBoss, you must make changes to the application server startup script. The startup script must be modified to specify JVM settings. For JBoss, you must also specify a log4j argument. For WebLogic 9, we recommend that you use the Administration Console to modify the WebLogic environment.

If you are using IBM WebSphere Application Server, SAP Web Application Server 6.40, or Oracle Application Server, no changes to its startup script are required unless you want to add the environment variable changes. If you do make changes, the Administrative Console can be used.

For Red Hat JBoss, we recommend that you create a copy of the default server instance so that you can use the original default server instance as a backup. Give the copy a name that does not use spaces, such as cognos.

If your environment contains a JRE that you are using for other products, the JRE folder may contain .jar files that are not compatible with the .jar files that are provided with Cognos 8. This may result in a failure to start Cognos 8 on your application server. In this situation, we recommend that you direct Cognos 8 to use the endorsed .jar files by including the following parameter in the Java command line:

`-Djava.endorsed.dirs=${cognos8_home}/tomcat[version]/common/endorsed`

Steps for WebLogic

1. Create a WebLogic Server (WLS) domain for Cognos 8.

   If you are configuring the Cognos Servlet Gateway, create a second domain for this application.

   For information about creating domains, see the WebLogic documentation.

2. Go to the appropriate directory and open the application server startup script in an editor. The following are possible directories:

   - *WebLogic8.1_location*/user_projects/domains/*domain_name*

- *WebLogic9_location*/user_projects/domains/*domain_name*/bin

The name of the startup script may vary depending on the type of WebLogic installation performed. For example, in a managed server installation, the name of the startup script is startManagedWebLogic.sh (UNIX) or startManagedWebLogic.cmd (Windows).

3. For non-IBM JRE versions, select the JVM run mode, and change the default setting from **JAVA_VM=** to **JAVA_VM=-server**

4. Modify the JAVA_OPTIONS to set the appropriate XML parser for Cognos 8. Add the third line, as shown in this example:

```
JAVA_OPTIONS=
-Dweblogic.security.SSL.trustedCAKeyStore=%WL_HOME%\server\lib\cacerts-Dorg.
xml.sax.driver=org.apache.xerces.parsers.SAXParser
```

5. Set the minimum and maximum memory used by the JVM.

   Typically, the memory is set using two JVM parameters: -Xms and -Xmx. A minimum of 256 MB and a maximum of 768 MB are suggested starting values. You can change these values to suit your environment.

   For WebLogic 9, the MaxPermSize parameter must also be set. Here is an example:

```
-XX:MaxPermSize=128m
```

   For information about JVM parameters, see the JVM or application server documentation.

6. Ensure that the production mode is enabled.

   For WebLogic 8 & 9, change **PRODUCTION_MODE=** to **PRODUCTION_MODE=true**

7. Save and close the file.

Steps for JBoss

1. Go to the *JBoss_location*/bin directory and open the application server startup script in an editor. Do one of the following:

   - For Windows, open run.bat
   - For UNIX or Linux, open run.sh

2. Go to the JAVA_OPTS variable and increase the memory used by the JVM.

   Typically, the memory is set using two JVM parameters: -Xms and -Xmx. A minimum of 256 MB and a maximum of 768 MB are suggested starting values. You can change these values to suit your environment.

   Here is an example:

```
rem Sun JVM memory allocation pool parameters. Modify
as appropriate.
set JAVA_OPTS=%JAVA_OPTS% -Xms192m -Xmx
768m -
Dsun.rmi.dgc.client.gcInterval=3600000 -
Dsun.rmi.dgc.client.gcInterval=3600000 -
```

   For information about these parameters, see the JVM or application server documentation.

3. Add a log4j argument, as shown in the following example:

```
rem Sun JVM memory allocation pool parameters. Modify
as appropriate.
set JAVA_OPTS=%JAVA_OPTS% -Xms256m -Xmx512m -
Dsun.rmi.dgc.client.gcInterval=3600000 -
Dsun.rmi.dgc.client.gcInterval=3600000 -
DLog4j.defaultInitOverride=true
```

For information about these parameters, see the JVM or application server documentation.

4. Save and close the file.

Change the Cognos Dispatcher Properties File for Oracle Application Server

If you are using Oracle Application Server, you must uncomment one entry in the Cognos dispatcher properties file. You must make this change before deploying Cognos components or problems will occur when running Cognos applications.

Steps

1. In a text editor, open the *c8_location*/webapps/WEB-INF/p2pd_deploy_defaults.properties file.
2. Locate the following entries:

```
#set this to true to wrap the input stream so
that Oracle Application Server will parse the XML properly
#wrap_input_stream=true
```

3. Uncomment the second entry by deleting the pound symbol (#), as shown here:

```
wrap_input_stream=true
```

4. Save and close the file.

Configure Application Server Properties and Deploy Cognos Components

You must configure application server properties and deploy the Cognos components.

Steps for WebSphere

1. Start the WebSphere Application Server, and then access the WebSphere Administrative Console.
2. Create a new server instance into which the Cognos 8 application will be deployed, if this option is available in the version you are running.

   If you are deploying the Cognos Servlet Gateway, create a second separate server instance.
3. Install a new Enterprise Application using the application file that was built by Cognos Configuration.

   For Cognos 8, the default context root is p2pd, which can be used in most cases. For the Cognos Servlet Gateway, the default context root is ServletGateway. Other default application

deployment values, such as the application name, may be changed to better suit your environment. The context root value used to deploy the application must be the same as the context root value entered in Cognos Configuration when running the Build Application wizard.

4. Set the memory used by the JVM.

   Usually, the memory is set by adding or changing the initial and maximum Java heap size. For information about these parameters, see the JVM or application server documentation.

   Tip: A minimum of 256 MB and a maximum of 768 MB are suggested starting values. You can change these values to suit your environment.

5. In the server properties, add an environment variable, as listed in the following table, that references the *installation_location*/bin directory.

Operating system	Environment variable
Windows	PATH
AIX	LIBPATH
Solaris	LD_LIBRARY_PATH
HP-UX	SHLIB_PATH

6. Stop and then restart the WebSphere application server instance used for Cognos components.
7. Verify that Cognos components are running by looking for the following message in the application server admin console or in the application server log file:

   The dispatcher is ready to process requests.

Steps for WebLogic

1. If you used the expanded directory option when building the application in Cognos Configuration, go to step 2. If you created a WAR file, expand the application manually:
   - Create a directory in a location that is accessible to the application server, giving the directory the same name as the context root.

     For Cognos 8, the default context root and application directory name is p2pd, which can be used in most cases. For the Cognos Servlet Gateway, the default context root is ServletGateway. Other default application deployment values, such as the application name, may be changed to better suit your environment. The context root value used to deploy the application must be the same as the context root value entered in Cognos Configuration.

   - From the directory you just created, extract the application WAR file to the WebLogic installation using the following command from a command prompt:

     WebLogic_location/jdk_version/bin/jar xvfm "installation_location/application.war" .

Important: A space and then a period are required at the end of the command. In this command, the period does not refer to the current directory.

2. Start the WebLogic Administration Server and the WebLogic Managed Server associated with the Cognos domain.

   Node Manager must be started before you can start and stop Managed Server instances using the Administration Console

3. For WebLogic 9, you must modify the environment in the WebLogic Administration Console before deploying Cognos 8. Logon to the Administration Console and navigate to the Managed Server instance that will host the Cognos 8 application. Select the **Server Start** tab for the Managed Server instance and enable edit mode.

4. In the **Java Home** box, enter the path for the JVM. This value must be the same as is used for Cognos 8. You must use the JVM that is included with the WebLogic installation.

5. Set the Java arguments.

   The Java arguments include all JVM settings, such as memory settings specified using two JVM parameters: -Xms and -Xmx. For WebLogic 9, the MaxPermSize must also be set. You must also set the appropriate XML parser for Cognos 8.

   For example, in the **Arguments** box, type

   -Xms768m -Xmx768m -XX:MaxPermSize=128m -Dorg.xml.sax.driver=org.apache.xerces.parsers.SAXParser

   If you use WebLogic Server 9 on AIX, you must also specify the appropriate serial version UID in the Java arguments. If you do not make this update, a serial version UID mismatch occurs when using WebLogic Server 9 with IBM Java 5 because WebLogic 9 requires JDK 1.5.

   For example, in the **Arguments** box, type

   -Xms768m -Xmx768m -XX:MaxPermSize=128m -Dorg.xml.sax.driver=org.apache.xerces.parsers.SAXParser -Dcom.sun.xml.namespace.QName.useCompatibleSerialVersionUID=1.0

   For information about JVM parameters, see the JVM or application server documentation.

6. Save and apply the changes.

   You can now start and stop the Managed Server instance from the **Control** tab.

7. Start the server instance. The server instance must be started before deploying Cognos 8 or or Cognos Servlet Gateway.

8. Deploy the Cognos 8 or Cognos Servlet Gateway application in the WebLogic console using a new Web application as follows:

   - Set the application name.

     For example, cognos8

   - Set the path to the directory where the expanded application files are located.

     Note: Cognos 8 uses a custom loader. You must use the expanded directory option when deploying.

- Select the target server instance.

  It is recommended that the Administration Server be used only for WebLogic administration tasks and that the Cognos 8 application be deployed to its own Managed Server instance.

9. After the deployment has completed successfully, set the reload period for the Web application to **-1** to improve performance. This will prevent WebLogic from checking for updated application files that are used only in a development environment.
10. Stop and then restart the WebLogic Managed Server associated with the Cognos domain to activate the changes.
11. Verify that Cognos components are running by looking for the following message in the application server console window or in the application server log file:

    The dispatcher is ready to process requests.

Steps for SAP Web Application Server 6.40 on Windows

1. Open the configuration tool by typing

   drive:\usr\sap\sapid\JCxx\j2ee\configtool\configtool.bat

   For example, if the SAP ID is J2E and the installation is on drive D, you would type

   D:\usr\sap\J2E\JC00\j2ee\configtool\configtool.bat
2. When prompted to use the default DB settings, click **Yes**.
3. Under **cluster-data**, **instance_IDxxxxxxx**, **Dispatcher_IDxxxxxxx**, **services**, where xxxxxxx is the ID number for your installation, highlight **http**.
4. Under **Global Properties**, highlight **KeepAliveTimeout** and type a higher number and then click **Set**.

   Tip: We suggest an initial **KeepAliveTimeout** number of at least 60.
5. Under **cluster-data**, **instance_IDxxxxxxx**, highlight **Server_IDxxxxxxx**.
6. Set the memory used by the JVM.

   Follow the recommendations from SAP. For more information, see SAP Note 723909 in the SAP Support Portal.

   If your computer has less than 1.5 GB of memory, you may have issues when you run SAP Web Application Server. We suggest a minimum value of 768 MB.
7. In the Java parameters box, set the XML parser as follows:

   -Dorg.xml.sax.driver=org.apache.xerces.parsers.SAXParser
8. For Cognos 8 environments that use Report Studio, under **cluster-data**, **instance_IDxxxxxxx**, highlight **Server_IDxxxxxxx**, **services**, and highlight **http**.
9. Under **Global Properties**, highlight **CompressedOthers**, type **false**, and then click **Set**.
10. Save the changes.

You are prompted to restart the server.

11. Restart the server by using the SAP Management Console or by restarting the services in Services.
12. Use the Deploy tool to create a new project.
13. Load the Cognos application file you created using Cognos Configuration. By default, the file is named p2pd.ear for Cognos 8 and ServletGateway.ear for Cognos Servlet Gateway.
14. Using the Deploy tool, connect to the Administration tool and deploy the application file.
15. When you are prompted to start the application, click **Yes**.
16. Save the project.

Steps for Oracle Application Server Release 2

1. Create an OC4J instance for Cognos components to run within.
2. Set the memory used by the JVM.

   Typically, the memory is set by adding or changing two JVM parameters: -Xms and -Xmx. A minimum of 256 MB and a maximum of 768 MB are suggested starting values. You can change these values to suit your environment. For information about these parameters, see the JVM or application server documentation.
3. In the server properties, add "-userThreads" to the OC4J Options.
4. In the server properties, add an environment variable, as listed in the following table, that references the *installation_location*/bin directory.

Operating system	Environment variable
Windows	PATH
AIX	LIBPATH
Solaris	LD_LIBRARY_PATH
HP-UX	SHLIB_PATH

5. Deploy the Cognos application file (named p2pd.ear for Cognos 8 or ServletGateway.ear for Cognos Servlet Gateway, by default) created by Cognos Configuration.

   The value of the Map to URL parameter must be the same as the context root value entered in Cognos Configuration.
6. Start the OC4J instance that you created for Cognos components.
7. Verify that Cognos components are running by looking for the following message in the application server console window or in the application server log file:

The dispatcher is ready to process requests.

Steps for Oracle Application Server Release 3

1. Create an OC4J instance for Cognos components to run within.
2. On Windows only, comment out the following entries in the *Oracle_location*\j2ee\ *Cognos_OC4J_instance*\config\global-web-application.xml file:

```
<welcome-file-list>
 <welcome-file>index.html</welcome-file>
 <welcome-file>default.jsp</welcome-file>
 <welcome-file>index.htm</welcome-file>
 <welcome-file>index.jsp</welcome-file>
   </welcome-file-list>
```

3. Open the *Oracle_location*/opmn/conf/opmn.xml file.
4. Add an environment variable that references the *installation_location*/bin directory and set variables for data sources.

   Here is an example for for Windows and DB2:

```
<environment>
 <variable id="PATH" value="c8_location/bin"
  append="true"/>
 <variable id="DB2DIR" value="
location"/>
 <variable id="DB2INSTANCE value="
instance_name"/>
 <variable id="INSTHOME value="
location"/>
</environment>
```

   This table lists the environment variables for each operating system that must reference the *c8_location*/bin directory.

Operating system	Environment variable
Windows	PATH
AIX	LIBPATH
Solaris	LD_LIBRARY_PATH
HP-UX	SHLIB_PATH

5. Set the memory used by the JVM.

   A minimum of 256 MB and a maximum of 768 MB are suggested starting values. You can change these values to suit your environment. For information about these parameters, see the JVM or application server documentation.

   Here is an example:

```
<data id="java-options" value="-server -Xmx768m -XX:MaxNewSize=384m
-XX:NewSize=192m -XX:MaxPermSize=128m -classpath
```

```
c8_location\bin;c8_location\webapps\p2pd\WEB-INF\lib
-
```

6. Define the OC4J userThreads setting.

   Here is an example:

   ```
   <data id="oc4j-options" value="-properties -userThreads"/>
   ```

7. Save and close the *Oracle_location*/opmn/conf/opmn.xml file.

8. Deploy the Cognos application file (named p2pd.ear for Cognos 8 or ServletGateway.ear for Cognos Servlet Gateway, by default) created by Cognos Configuration.

   The value of the Map to URL parameter must be the same as the context root value entered in Cognos Configuration.

9. Start the OC4J instance that you created for Cognos components.

10. Verify that Cognos components are running by looking for the following message in the application server console window or in the application server log file:

    The dispatcher is ready to process requests.

Steps for JBoss

1. If you do not want to use the default port of 8080, open the *JBoss_location*/server/*instance_name*/deploy/jbossweb-tomcat55.sar/server.xml file.

2. In the server.xml file, change the default port number of 8080 used by the server instance to the port specified in Cognos Configuration. For example,

   ```
   <Service name="jboss.web"
    className="org.jboss.web.tomcat.tc5.StandardService">
   <!-- A HTTP/1.1 Connector on port 8080 -->
   <Connector port="8080" address="${jboss.bind.address}"
    maxThreads="250" strategy="ms" maxHttpHeaderSize="8192"
    emptySessionPath="true"
    enableLookups="false" redirectPort="8443" acceptCount="100"
    connectionTimeout="20000" disableUploadTimeout="true"/>
   ```

3. Save and close the server.xml file.

4. Put the p2pd application in the *JBoss_location*/server/*instance_name*/deploy folder, if it is not already in this location.

5. Start the application server.

   The p2pd application is automatically detected and started by the application server.

6. Verify that Cognos components are running by looking for the following message in the application server console window or in the application server log file:

   ```
   The dispatcher is ready to process requests.
   ```

Enable SSL

If you use the Secure Socket Layer (SSL) for Cognos components, you must also enable SSL in the application server environment. You then identify the SSL server certificate to Cognos components.

Steps

1. Configure the application server to use SSL.

   An SSL server certificate is generated by a third-party Certificate Authority (CA). The certificate of the CA that generated the SSL server certificate is also provided.

   For more information about configuring the application server to use SSL, refer to the application server documentation. For information about using CA certificates with your application server, see the CA documentation.

2. Copy the CA certificate to the *installation_location*/bin directory and rename the file to ca.cer.

   This file must be Base-64 encoded X.509 format.

3. From the *installation_location*/bin directory:

   - On Windows, type:

     ThirdPartyCertificateTool.bat -T -i -r ca.cer -k ../configuration/signkeypair/jCAKeystore -p *password*

   - On UNIX or Linux, type:

     ThirdPartyCertificateTool.sh -T -i -r ca.cer -k ../configuration/signkeypair/jCAKeystore -p *password*

   Important: You must type jCAKeystore as the name of the CA key store.

Configuring the Web Server

If you are using a Web server in your environment, configure it now. For information about configuring the web server, see "Configure the Web Server " (p. 132).

For information about configuring the WebSphere Web server plugin, contact Cognos Customer Support (http://support.cognos.com).

Unregister Dispatchers

After you start the application server and the Cognos application, unregister any Cognos dispatchers that were previously registered and that are no longer used. For example, unregister any Tomcat dispatchers that are now running under the application server.

You remove dispatchers using Cognos Administration. To access this tool, you must have execute permissions for the Administration secured function.

Steps

1. Open Cognos Connection.
2. In the upper-right corner, click **Launch**, **Cognos Administration**.
3. On the **Configuration** tab, click **Dispatchers and Services**.
4. For the dispatcher you want to unregister, from the **Actions** column, click **More**.
5. Click **Unregister**.
6. In the confirmation dialog, click **OK**.

The dispatcher information is removed from Content Manager.

Import Content Store Data

If you exported the content store before setting up Cognos components to run in your application server (p. 295), import the deployment to restore and encrypt the data using the new encryption keys.

Step

1. Start Cognos 8.
2. Import the entire content store using the Deployment tool.

   For more information, see the topic about importing to a target environment in the *Administration and Security Guide*.

Upgrade to Cognos 8 in an Application Server Environment

If you are upgrading from a supported release to Cognos 8, perform the following steps.

Steps

1. Back up your existing Cognos information (p. 295).
2. Use the administrative tools for your application server to undeploy the existing Cognos application.

   For information about undeploying applications, see your application server documentation.

   If the directory to which the existing Cognos application was originally deployed is not removed during the undeploy process, delete the directory.

   Also, remove any Cognos .jar files that are cached in your application server environment.

In WebLogic 8.1, the cache location is %WL_HOME%\user_projects\domains*domain-name**managed-server-name*\.wlnotdelete\extract\crn_p2pd_p2pd\ jarfiles

3. Uninstall the existing version. (p. 113).
4. Install Cognos 8 (p. 93).
5. Follow the appropriate instructions in this chapter for changing to your application server.

   Most installations must perform the following:

   - Configure Cognos 8 to run within the application server.
   - Configure application server properties and deploy Cognos 8.
6. To activate new features after upgrading, save the configuration in Cognos Configuration, and then restart the services.

Upgrade from Metrics Manager to Cognos 8 in an Application Server Environment

If you are upgrading from Metrics Manager to Cognos 8, perform the following steps.

Steps

1. Follow the procedure to upgrade Metrics Manager to Cognos 8 (p. 72).
2. Follow the appropriate instructions in this chapter for changing to your application server.

   Most installations must perform the following:

   - Configure Cognos 8 to run within the application server.
   - Configure application server properties and deploy Cognos 8.
3. To activate new features after upgrading, you must save the configuration in Cognos Configuration, and then restart the services.

Chapter 13: Advanced Configuration Options

Advanced configuration options are changes that you make after installation to the configuration properties of the resources that Cognos 8 components use. You cannot use Cognos Configuration to make these changes. Advanced configuration options enhance security, improve performance, or change the default behavior of Cognos 8 components.

Change the Type of JVM Used by Cognos 8

To better suit your reporting environment, you can change the type of Java Virtual Machine (JVM) that Cognos 8 components use, based on the following criteria:

- Java HotSpot Client VM

  Use this JVM for proof of concept, demonstration, or development environments. This JVM is specially tuned to reduce both the startup time for applications and the memory footprint.

  This is the default setting for Cognos installations on Windows. On UNIX and Linux platforms, Cognos does not provide a Java Runtime Environment (JRE). Therefore, the default JVM that Cognos 8 components use depends on the current setting in your existing JRE.

- Java HotSpot Server VM

  Use this JVM for long-running server applications to maximize operating speeds when performance is more important than fast startup time.

For more information, see the Sun Microsystems Inc. Web site.

Steps

1. Go to the location where your Java Runtime Environment (JRE) libraries are installed:
   - In Windows, go to *c8_location*\bin\jre*jre_version*\lib\i386.
   - In UNIX or Linux, go to JAVA_HOME/jre/lib.
2. Open jvm.cfg in an editor.
3. Ensure that the JVM that you want to use is the first uncommented line. Enter the appropriate text for the JVM you want to use:

JVM	Text
Hotspot Client	hotspot
Hotspot Server	server

4. Save and close the file.

Changing the Version of Java Runtime Environment Used by Cognos 8 Components

Cognos 8 components require Java Runtime Environment (JRE) to operate. The current version provided with Cognos 8 is JRE 1.5.0. For more information about the supported JRE versions, see the Cognos Support Website (http://support.cognos.com).

Cognos Configuration and other Cognos 8 components use the JRE referenced by the JAVA_HOME environment variable. On Windows, if JAVA_HOME is not set, the JRE that is packaged with Cognos 8 components is used by default.

If you want to change your current JRE, some configuration changes are required. Changing may be appropriate in the following situations:

- You want to use Cognos 8 components with an application server that requires a specific JRE version.
- You already use a JRE version with other applications.

If you are using Cognos 8 components in an application server environment, follow the process in "Configuring Cognos 8 for a Third-Party Application Server" (p. 293). The process includes steps for updating the Java environment.

Before you begin, ensure that Cognos 8 components are installed and that JRE you want to use is installed.

To change JRE versions, do the following:

- ❑ Back up existing Cognos data and encryption keys, if required.
- ❑ Updated the Java environment.
- ❑ Import data to the content store, if required.

The tasks in this section are for a Cognos installation that uses Tomcat.

Back Up Existing Cognos Information

You must back up existing Cognos information if Cognos 8 components are running

- on an application server (including Tomcat) and you are changing to an application server that ships with its own JVM.
- with a JVM from one vendor and you are changing to another JVM vendor.

Note: You must back up existing Cognos information within the working environment prior to upgrade.

Before configuring Cognos 8 components to run on the new application server or JVM, you must back up

- content store data by creating a deployment export.
- configuration information by exporting it. Any encrypted data is decrypted during the export.
- cryptographic keys by saving them to an alternate location. New cryptographic keys must be created using the same JVM that the application server uses. Because these keys can be created only if the previous keys are deleted, it is important to back up the previous keys.

To ensure the security and integrity of your Cognos data, back up the content store, configuration information, and cryptographic keys to a directory that is protected from unauthorized or inappropriate access.

Tip: To check if any cryptographic keys exist, look in the *c8_location*/configuration directory. Cryptographic keys exist if this directory includes the following subdirectories: csk, encryptkeypair or signkeypair.

Steps

1. If data exists in the content store, start the Cognos 8 service and export the entire content store using the Deployment tool.

   For more information, see the topic about creating an export deployment specification in the *Administration and Security Guide*.

2. In Cognos Configuration, from the **File** menu, click **Export As** and save the configuration information in a decrypted format. When naming the file, use a name such as "decrypted.xml".

   Export the data to a directory that is protected from unauthorized or inappropriate access because passwords are stored in plain text. You are prompted to acknowledge that the export is an unsecure operation.

3. Stop the Cognos 8 service:
   - If you use Tomcat, stop the Cognos 8 service and close Cognos Configuration.
   - If you use an application server other than Tomcat, shut down Cognos 8 in your environment.

4. Back up any existing cryptographic keys by saving the appropriate files and directories to an alternate location that is secure.

   The files are
   - *c8_location*/configuration/cogstartup.xml
   - *c8_location*/configuration/caSerial
   - *c8_location*/configuration/cogconfig.prefs
   - *c8_location*/configuration/coglocale.xml

   The directories are
   - *c8_location*/configuration/csk
   - *c8_location*/configuration/encryptkeypair

- *c8_location*/configuration/signkeypair

5. Delete the caSerial and cogconfig.prefs files and the three directories: csk, encryptkeypair, and signkeypair.
6. Replace the *c8_location*/configuration/cogstartup.xml file with the file that contains the data exported from Cognos Configuration (for example, "decrypted.xml").

   Important: In the *c8_location*/configuration directory, the file must use the name "cogstartup.xml".

   The information in this file will be automatically re-encrypted using new cryptographic keys when you save the configuration in Cognos Configuration.

Update the Java Environment

The Cognos security provider files must be located in the JVM environment for the new version of Java.

Cognos 8 cryptographic services use a specific .jar (Java Archive) file, named bcprov-jdk*nn-nnn*.jar, that must be located in your Java Runtime Environment (JRE). This file provides additional encryption and decryption routines that are not supplied as part of a default JVM installation. To ensure security, the encryption file must be loaded by the JVM using the java extensions directory.

If you want to use your own JRE and have JAVA_HOME set to that location on Windows or if you are installing on UNIX, you may have to update the Java environment for the cryptographic services.

On Windows, you can set JAVA_HOME as a system variable or a user variable. If you set it as a system variable, it may be necessary to restart your computer for it to take effect. If you set it as a user variable, set it so that the environment in which Tomcat is running can access it.

If you do not have a JAVA_HOME variable already set on Windows or if JAVA_HOME points to a Java version that is not valid for Cognos 8, the JRE files provided with the installation will be used, and you do not have to update any files in your environment.

Steps

1. Ensure that the JAVA_HOME environment variable is set to the JRE location.

   For example, to set JAVA_HOME to the JRE files provided with the installation, the path is *c8_location*/bin/jre/*version*.

2. Copy the bcprov-jdk*nn-nnn*.jar file from the *c8_location*/bin/jre/*version*/lib/ext directory to the *Java_location*/lib/ext directory.
3. Start Cognos Configuration.
4. Save the configuration.

   Cognos Configuration generates new keys and encrypts the data.

Import Content Store Data

If you exported the content store before changing the JVM, import the deployment to restore and encrypt the data using the new encryption keys.

Step

- To import the content store data, start the Cognos 8 service and import the entire content store using the Deployment tool. For more information, see the topic about importing to a target environment in the *Administration and Security Guide*.

Configuring Cognos 8 Components to Use a Third-party Certificate Authority

By default, Cognos 8 components use their own certificate authority (CA) service to establish the root of trust in the Cognos security infrastructure. You can configure Cognos 8 components to use another certificate authority, if you already have an existing third-party certificate authority, such as iPlanet or Microsoft, in your reporting environment.

When you configure Cognos 8 components to use a third-party certificate authority, ensure that you specify the same information in both the command line utility tool and in Cognos Configuration.

To configure Cognos 8 components to use your third-party certificate authority, you must

- ❑ generate Cognos security keys and certificate signing requests to use with your third-party CA
- ❑ submit the Cognos security keys and certificates to your third-party certificate authority
- ❑ configure Cognos 8 components to use a third-party certificate authority

Generate Keys and Certificate Signing Requests

Use the command line utility to generate all the keys for the Cognos key stores and to generate the certificate signing requests (CSR).

The following table lists the options for the command-line tool used to generate keys and signing requests.

Command	Description
Main operation mode	
-c	Create a new CSR
-i	Import a certificate
Operation modifiers	

Command	Description
-s	Work with the signing identity
-e	Work with the encryption identity
-T	Work with the trust store (only with -i)
Information Flags	
-d	DN to use for certificate
-r	CSR or certificate file location (depends on mode)
-t	certificate authority certificate file (only with -i)
-p	Key Store password (must be provided)
-a	Key pair algorithm. RSA or DSA. **Default:** RSA
-D	Directory location

The following sample values are used:

Property	Value
Signing certificate DN	CN=SignCert,O=MyCompany,C=CA
Encryption certificate DN	CN=EncryptCert,O=MyCompany,C=CA
Key store password	password

Steps

1. In the *c8_location*\configuration directory, back up the cogstartup.xml file to a secure location.
2. Back up the contents of the following directories to a secure location:
   - *c8_location*\configuration\signkeypair
   - *c8_location*\configuration\encryptkeypair
3. Using Cognos Configuration, export the configuration in clear text by doing the following:
   - Open Cognos Configuration.
   - From the **File** menu, click **Export As**.

- When prompted about exporting decrypted content, click **Yes**.
- In the **Export As** dialog box, select cogstartup.xml and then click **Save**.
- When prompted about replacing the existing file, click **Yes**.
- When the tasks are complete, close the Cognos Configuration dialog box.
- Save the configuration.
- Close Cognos Configuration.

4. Go to the *c8_location*\bin directory.
5. Create the certificate signing request for the signing keys by typing the following command:

   On UNIX or Linux, type

   ThirdPartyCertificateTool.sh -c -s -d "CN=SignCert,O=*MyCompany*,C=CA" -r signRequest.csr -D ../configuration/signkeypair -p *password*

   On Windows, type

   ThirdPartyCertificateTool.bat c -s -d "CN=SignCert,O=*MyCompany*,C=CA" -r signRequest.csr -D ../configuration/signkeypair -p *password*

   Tip: UNIX or Linux filenames are case-sensitive and must be entered exactly as shown.

   You can safely ignore any warnings about logging.

   The command creates the jSignKeystore file in the signkeypair directory, sets the specified password, creates a new keypair and stores it in the keystore, and exports the signRequest.csr file to the *c8_location*\bin directory.
6. Create the certificate signing request for the encryption keys by typing the following command:

   On UNIX or Linux, type

   ThirdPartyCertificateTool.sh -c -e -d "CN=EncryptCert,O=*MyCompany*,C=CA" -r encryptRequest.csr -D ../configuration/encryptkeypair -p *password*

   On Windows, type

   ThirdPartyCertificateTool.bat -c -e -d "CN=EncryptCert,O=*MyCompany*,C=CA" -r encryptRequest.csr -D ../configuration/encryptkeypair -p *password*

   You can safely ignore any warnings about logging.

   The command creates the jEncKeystore file in the encryptkeypair directory, sets the specified password, creates a new keypair and stores it in the keystore, and exports the encryptRequest.csr file to the *c8_location*\bin directory.
7. Copy the signRequest.csr and encryptRequest.csr files that were generated in steps *5* and *6* to a directory that is accessible by your third-party certificate authority.
8. Input the signRequest.csr and encryptRequest.csr files into the third-party certificate authority.

   The certificate authority produces a signing certificate and an encryption certificate.

   For more information, see your third-party CA documentation.

9. Copy the contents of the signing certificate into a file named signCertificate.cer.
10. Copy the contents of the encryption certificate into a file named encryptCertificate.cer
11. Find the root CA certificate for the certificate authority and copy the contents into a file named ca.cer.
12. Copy ca.cer, signCertificate.cer, and encryptCertificate.cer to *c8_location*/bin.

    These files must be PEM (Base-64 encoded ASCII) format.
13. Import the signing certificate from step 10 into the Cognos signing key store by typing the following command:

    On UNIX or Linux, type

    ThirdPartyCertificateTool.sh -i -s -r signCertificate.cer -D ../configuration/signkeypair -p *password* -t ca.cer

    On Windows, type

    ThirdPartyCertificateTool.bat-i -s -r signCertificate.cer -D ../configuration/signkeypair -p *password* -t ca.cer

    You can safely ignore any warnings about logging.

    The command reads the signCertificate.cer and ca.cer files in the c8_location\bin directory and imports the certificates from both files into the jSignKeystore file in the signkeypair directory using the specified password.
14. Import the encryption certificate from step 11 into the Cognos encryption key store by typing the following command:

    On UNIX or Linux, type

    ThirdPartyCertificateTool.sh -i -e -r encryptCertificate.cer -D ../configuration/encryptkeypair -p *password* -t ca.cer

    On Windows, type

    ThirdPartyCertificateTool.bat -i -e -r encryptCertificate.cer -D ../configuration/encryptkeypair -p *password* -t cacert.cer

    You can safely ignore any warnings about logging.

    The command reads the encryptCertificate.cer and ca.cer files in the c8_location\bin directory and imports the certificates from both files into the jEncKeystore file in the encryptkeypair directory using the specified password.
15. Import the CA certificate from step 12 into the Cognos trust store by typing the following command:

    On UNIX or Linux, type

    ThirdPartyCertificateTool.sh -i -T -r ca.cer -D ../configuration/signkeypair -p *password*

    On Windows, type

    ThirdPartyCertificateTool.bat -i -T -r ca.cer -D ../configuration/signkeypair -p *password*

The command reads the ca.cer file and imports the contents into the jCAKeystore file in the signkeypair directory using the specified password.

The certificates are now ready to be configured for Cognos 8.

Configure Cognos 8 Components to Run Within a Third-party Certificate Authority

You must configure each Cognos computer to use an external certificate authority by setting the appropriate property in Cognos Configuration.

By setting this property, Cognos 8 components assume that all required keys have been generated and vetted by the external certificate authority.

Ensure that the key store locations and password in Cognos Configuration match the ones you typed in the command-line tool.

Steps

1. Start Cognos Configuration.
2. In the **Explorer** window, under **Security**, **Cryptography**, click **Cognos**.
3. In the **Properties** window, under **Certificate Authority settings** property group, click the **Value** box next to the **Use third party CA** property and then click **True**.

   Note: When you set this property to true, all properties for the certificate authority and identity name are ignored.
4. Configure the following properties to match the ones you typed in the command line utility:
   - **Signing key store location**
   - **Signing key store password**
   - **Encryption key store location**
   - **Encryption key store password**
   - **Certificate Authority key store password**
5. From the **File** menu, click **Save**.
6. If you want to start the Cognos 8 service, from the **Actions** menu, click **Start**.

   This action starts all installed services that are not running. If you want to start a particular service, select the service node in the **Explorer** window and then click **Start** from the **Actions** menu.

Chapter 14: Samples

This section explains the purpose, content and location of Cognos 8 samples. It also discusses the sample company, Great Outdoors, its structure, databases, model and packages.

For information on how to set up the sample databases, see "Setting Up the Samples" (p. 328).

Great Outdoors Samples

The Great Outdoors samples illustrate product features and technical and business best practices. You can also use them for experimenting with and sharing report design techniques, and for troubleshooting.

For examples related to different kinds of businesses, see the product blueprints on the Cognos Web site (http://www.cognos.com). For information about specific installation choices and environments, see the *Architecture and Deployment Guide*, or the Proven Practices and the Cognos Implementation Roadmaps on the Cognos Global Customer Services Web site (http://support.cognos.com). For information about audit samples, see the *Administration and Security Guide*.

Where to Find the Samples

The samples are included with the product and the samples for each studio are described in the related user guide and online help. To use the samples, you must set up and configure them, or contact your administrator to find out where they are installed. For instructions on how to set up and configure samples, see the *Installation and Configuration Guide* or the *Administration and Security Guide*.

What Samples Exist

The samples consist of

- two databases that contain all corporate data, the related sample models for query and analysis, and sample cubes, reports, queries, query templates, and dashboards
- a metrics database and the associated metrics, including a strategy map for the consolidated company

  Note: You must have Metric Studio installed to use these samples.
- reports that contain extended tips to explain how and why they were created

  Note: These reports are stored in a folder labeled Practical Examples in the samples folder of the Cognos 8 installation.

Security

You can add security to the samples using an employee list included with the product. The list is in the form of an LDIF file that can be imported into any directory server, such as the Sun Java System Directory Server.

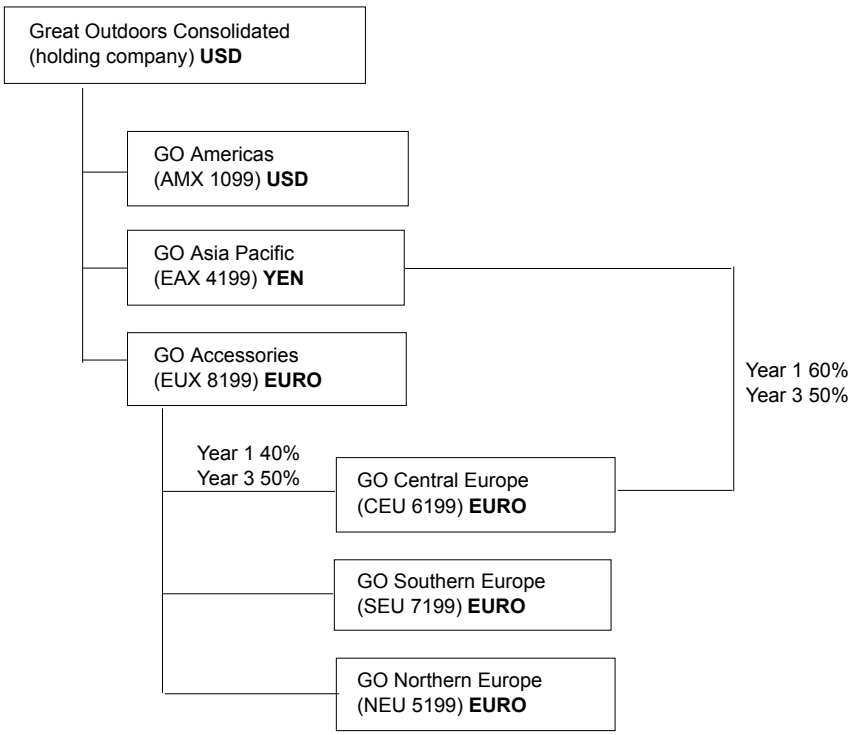
Note: You can download a version of the Sun Java System Directory Server from the Sun Web site (http://www.sun.com/download/). For more information, see the *Installation and Configuration Guide*. For information about conformance, see the Cognos Global Customer Services Web site (http://support.cognos.com).

The Great Outdoors Group of Companies

To make designing examples faster, especially financial examples, some general information about the fictional Great Outdoors company is useful. To look for samples that use particular product features, see the individual sample descriptions in this appendix.

Revenue for The Great Outdoors comes from corporate stores and from franchise operations. The revenues are consolidated from the wholly-owned subsidiaries. The corporate structure is shown below.

The diagram below illustrates the consolidated corporate structure, including the percentage changes in ownership for GO Central Europe, and shows the reporting currency and GL prefix for each subsidiary.



Each corporation has the same departmental structure and the same GL structure, shown in the table below. Divisions may not report in the same currencies. For example, the Americas subsidiary reports in US dollars, but the Corporate division local currency is Canadian dollars, and the Operations division local currency is pesos.

Division (GL)	Department (GL)
Corporate division (1700)	Sales (1720)
	Marketing (1750)
	IS&T (1760)
	Human Resources (1730)
	Finance (1740)
	Procurement (1710)
Operations (1800)	Production and Distribution (1820)
	Customer Service (1820)

Employees

The Great Outdoors data contains a full list of employees in all divisions, departments, and locations. Data is available for reports about bonuses (Global Bonus report) and sales commissions (Sales Commissions for Central Europe report), training (Employee Training by Year report), and performance reviews and employee satisfaction surveys (Employee Satisfaction 2006). If you use Metric Studio, sample metrics for human resources are also available.

In the GO Data Warehouse (analysis) package, groups of measures and the related dimensions are organized into folders. The employees are organized in hierarchies for region, manager, position or department, and organization, to make different kinds of aggregation easy to report on. Aggregation has been set for the Employee Position Summary measures, so that Position count and Planned position count aggregate to a maximum for time dimensions, and a sum for other dimensions. For example, see the Planned Headcount report.

The employees are also listed in a sample LDIF file (p. 324). This authentication directory is necessary for the Transformer 8 cubes and for Cognos Planning samples. No other samples depend on security profiles. For more information, see the *Installation and Configuration Guide*.

Sales and Marketing

Data about sales and marketing is available for all of the companies in the Great Outdoors group. GO Accessories has richer details to support analysis examples. For example, see the Revenue vs % Gross Profit by Product Brand analysis, based on the Sales and Marketing cube. Marketing and sales campaigns are tied to the Great Outdoors regional companies.

Overall, the GO companies have experienced solid growth across most product lines (Sales Growth Year Over Year), in all regions (Revenue by GO Subsidiary 2005), because of factors like an increase in repeat business and new or improved products, such as the high margin sunglasses product line. In the product lines sold by the five regional companies (all but GO Accessories) promotions have had mixed success (Promotion Success by Campaign, Bundle and Quarter). If you use Metric Studio, this can also be seen in the sample metrics.

Customer Surveys

The data also contains information from customer surveys. For example, the product line that includes bug spray, sun screen, and so on has not been successful (Product Satisfaction - Outdoor Protection 2005) and a source of retailer dissatisfaction may be the level of customer service rather than the returns (Customer Returns and Satisfaction). If you use Metric Studio, this information can also be monitored in metrics.

Sales Outlets

Revenue from the corporate outlets is available at the transaction level. Revenue from the franchise outlets is available at the consolidated level only (Sales and Marketing cube). Metrics about retailers show that the number of new retail outlets has dropped over the time period covered by this data.

GO Accessories sells worldwide, and sells only accessories. The other five subsidiaries in the group of companies are regional and sell all product lines for retailers in their region. For example, the report Top 10 Retailers in 2005 uses sparklines and list data to review revenues at the retailer level.

Great Outdoors Database, Models, and Packages

The Great Outdoors models illustrate modeling techniques and support the samples. The models are based on the GO data warehouse and the GO sales transactional database and are the basis for the sample reports and queries. Each model contains two packages for publishing analysis (dimensional) and query views of the data.

For a description of each sample report or query, see the user guide for the studio that you open the sample in. For more information about modeling techniques, see the *Guidelines for Modeling Metadata*, or the Framework Manager *User Guide*.

You must have access to Framework Manager, the modeling tool in Cognos 8, to look at the sample models. You may also need to set up the sample databases and connections. For instructions, see the *Administration and Security Guide* or the *Installation and Configuration Guide*.

GO Data Warehouse

The GO Data Warehouse model, great_outdoors_data_warehouse.cpf, is based on the database GOSALESDW. It contains data about human resources, sales and marketing, and finance, grouped into business areas. In the Database view, the three business areas are grouped into separate namespaces. The Database view contains a fourth namespace (GO Data) for the common information.

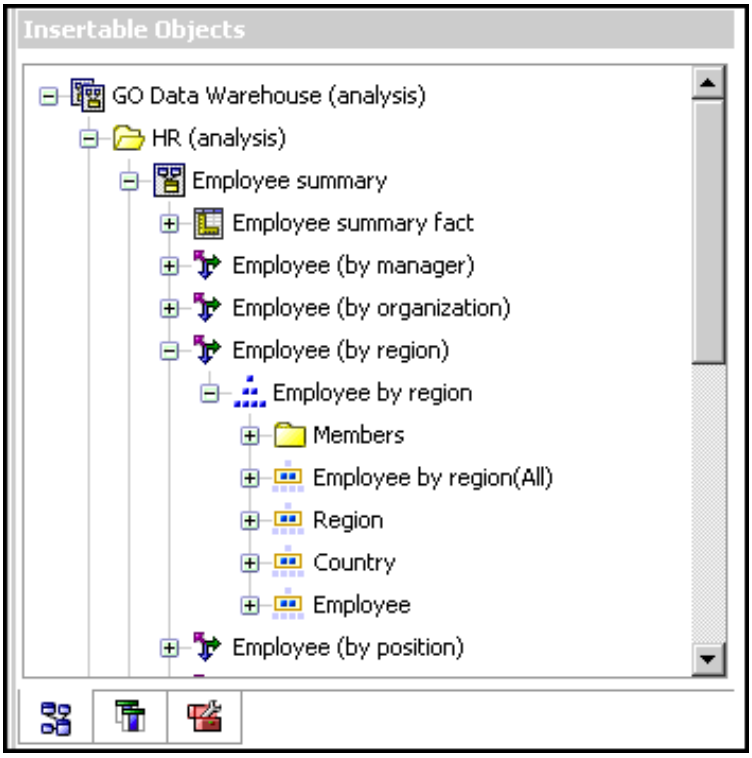
The Database view is very similar to the structure of the underlying database. All tables (database query subjects) are unchanged. This enables Cognos 8 to retrieve metadata directly from the package

in most cases, instead of using a metadata call to the database. The following changes and additions have been made in the Database view:

- Joins have been added as necessary.
- To allow for aggregation at different levels of granularity, some model query subjects have been created. For example, see the relationships between Time and Sales or Sales fact.
- To allow single joins to be made between the lookup tables and each level in a dimension, lookup tables have been copied. For example, see the Products look up tables.

The Business view contains only model query subjects, with no joins. The following changes and additions have been made in the Business view:

- Calculations were added to the model query subjects. For example, the time dimension contains language calculations.
- Where the database has multiple hierarchies, new dimensions have been created to organize each hierarchy. For example, see the employee hierarchies, where employees are organized by manager, organization, region, and position.



The GO Sales Transactional Database

The GO Sales model, great_outdoors_sales.cpf, is based on the GOSALES database, which is structured as a transactional database. It contains principally sales data.

The Database view is very similar to the underlying database structure. The following changes and additions have been made in the Database view:

- To make it possible to join the fact tables to the time dimension, model query subjects and multipart joins have been used.

- Other joins have been added as necessary.

The Business view contains only model query subjects, with no joins. The following changes and additions have been made in the Business view:

- Calculations were added to the model query subjects.
- Model query subjects that were created in the Database view to enable joins on the time dimension have been linked as reference shortcuts.
- Where the database has multiple hierarchies, new dimensions have been created to organize each hierarchy.
- Slowly changing dimensions require calculations to ensure that the correct record for the time period is retrieved. This is done with a calculation such as the one shown below, for the relationship between Sales Staff and Orders.

```
[Business view].[Sales
Staff].[Sales staff code]=[Business view].[Sales].[Sales staff code]
and ([Business view].[Sales].[Day key (order date)] between [Business
view].[Sales Staff].[Day key (record start date)]  and [Business
view].[Sales Staff].[Day key (period record end date)] )
```

Setting Up the Samples

You can use the Cognos samples to learn how to use Cognos 8, including Framework Manager, Metric Studio, Metric Designer, and Event Studio.

Cognos 8 provides sample databases that contain sales, marketing, and financial information for a fictional company named the Great Outdoors Company that sells sporting equipment.

Before you can use the sample databases, Cognos 8 must be installed, configured, and running. For Cognos 8 reports and analyses, Framework Manager should also be installed, configured, and running.

To use the sample content for Metric Designer, the optional modeling tool for Metric Studio, Metric Designer must also be installed, configured, and running.

To set up the samples, do the following:

- ❑ Restore the samples databases.
- ❑ Create the data source connections to the samples databases.
- ❑ If you plan to use OLAP data source samples, set up the sample cubes, if this is required, and create data source connections to the OLAP data sources you want to use.

  Setup tasks are required only for Microsoft Analysis Services cubes and DB2 cubes.
- ❑ If you plan to use the Metric Studio sample, set up the Metric Studio sample.
- ❑ If you plan to use the Metric Designer sample, set up a data source connection to it, set up the Metric Studio sample, and import the Cognos_Samples and GO_Metrics deployment archives.
- ❑ Import the samples content (packages) into the content store.

- If you want to test the sample agent ELM Returns Agent using Event Studio, run the sample agent against changed data.

After you complete these tasks, use Cognos 8 to run the sample reports or scorecards. You can later remove the Cognos 8 samples.

Restore Backup Files for the Samples Databases

To use the samples, you must restore backup files for the samples databases. This action re-creates multilingual versions of the Great Outdoors databases.

The following sample databases and associated files are provided with Cognos 8. For SQL Server and Oracle, each database is delivered as a Microsoft SQL Server backup file and an Oracle export file (.dmp). For DB2, the database schemas are delivered in a DB2 move file. The file are compressed, and you must extract them before you can restore the databases or schemas.

Database or schema description	SQL Server	Oracle	DB2
Great Outdoors sales	GOSALES.zip	GOSALES.dmp.gz	GS_DB.tar.gz
Great Outdoors retailers	GOSALES.zip	GOSALESRT Restore Backup Files .dmp.gz	GS_DB.tar.gz
Great Outdoors sales data warehouse	GOSALESDW. zip	GOSALESDW. dmp. gz	GS_DB.tar.gz
Great Outdoors market research	GOSALES.zip	GOSALESMR. dmp. gz	GO_DB.tar.gz
Great Outdoors human resources	GOSALES.zip	GOSALESHR. dmp. gz	GO_DB.tar.gz

When restoring the samples databases, ensure that you do the following:

- Give the restored databases the same names as the backup or export file names.

  The names are case-sensitive.

- Create a user in your database who has select privileges for all schemas.

  The GO Sales package references tables in all schemas.

- Use the UTF-8 character set.

- Have sufficient disk space available in the target location. Reserve 150MB for the GO Sales data (four schemas) and 200MB for the GO Sales warehouse data (one schema).

Oracle Considerations

To create foreign key constraints in tables that reference different schemas, you must run ora_gosales.sql, found in the same folder as the .dmp files.

SQL Server Considerations

If you restore the SQL Server backup files, you must use Microsoft SQL Server 2000 or Microsoft SQL Server 2005. Ensure that TCP/IP connectivity is used for the SQL server.

DB2 Considerations

Before you restore the Great Outdoors schemas contained in the DB2 move file on UNIX or Windows, extract the DB2 move file. On UNIX, extract the DB2 move file using the *gnutar -xcvf DB2_move_filename* or *tar -xcvf DB2_move_filename* command. If you use WinZip to extract the DB2 move file on Windows, ensure that the TAR file smart CR/LF conversion option is not selected.

After extracting the DB2 move file, restore the schemas to a database named GS_DB. When you create this database in DB2, create a buffer pool with a page size of 16 KB and an associated tablespace.

To restore schemas to the GS_DB database, you must edit the gs_db_modify.sql file and enter a user name and password in the file. You must also run the gs_db_modify.bat file to create additional views and constraints in the GS_DB database.

Steps

1. On the computer where Cognos 8 is installed, go to the sql server, oracle, or db2 directory located in *c8_location* /webcontent/samples/datasources.
2. If required, copy the backup files for the samples databases to your database backup directory.

   To ensure the security and integrity of Cognos 8, copy the files to a directory that is protected from unauthorized or inappropriate access.
3. Restore the samples databases using your database management tool.

   Tip: For SQL backup files, restore the database from a device and ensure that the restore locations are correct for the .ldf and .mdf database files. For more information, see the Microsoft SQL Server documentation or the Cognos Knowledge Base (http://support.cognos.com/kb-app/knowledgebase).
4. For each database, create at least one user who has select permissions for all the tables in the restored databases.

You can now create the data source connections in the portal.

Create Data Source Connections to the Samples Databases

You must create data source connections to the samples databases that you restored. Cognos 8 uses this information to connect to the samples databases and run the sample reports or use the sample package.

The DB2 database name that you type must use uppercase letters. Also, in Framework Manager, the schema names that you type for the DB2 data sources must use uppercase letters.

Before you create the data source connections, you must restore the backup files for the samples databases. Also, ensure that the Cognos 8 service is running.

To create data sources, you must have execute permissions for the Directory secured feature and traverse permissions for the Administration secured function.

Steps

1. Open Cognos Connection.
2. In the upper-right corner, click **Launch**, **Cognos Administration**.
3. On the **Configuration** tab, click **Data Source Connections**.
4. Click the new data source button .
5. In the **Name** box, type **great_outdoors_sales** and then click **Next**.
6. In the connection page, click the type of database that you restored and want to connect to, select an isolation level, and then click **Next**.

   The connection string page for the selected database appears.

   Tip: The user specified in the great_outdoors_sales data source must have select privileges on the tables in each of the GOSALES, GOSALESRT AND GOSALESHR schemas (p. 329).
7. Do one of the following:
   - If you restored the samples databases in SQL Server, in the **Server Name** box, type the name of the server where the restored databases are located. In the **Database name** box, type **GOSALES**.

     Cognos 8 samples require TCP/IP connectivity with SQL Server. Ensure the SQL Server Security is set to SQL Server and Windows, instead of Windows Only. The samples use SQL Server security for authentication.
   - If you restored the samples databases in Oracle, in the **SQL*Net connect string** box, type the Oracle connection string.
   - If you restored the samples database in DB2, in the **DB2 database name** box, type **GO_DB** using uppercase letters. In the **DB2 connect string** box, type the DB2 connection string.
8. Under **Signons**, select the **Password** and **Create a signon that the Everyone group can use** check boxes, type the user ID and password for the user that you created when you restored the databases, and then click **Finish**.

   Tip: To test whether the parameters are correct, click **Test**.
9. Click **Finish**.
10. Repeat steps 4 to 9 for the GOSALESDW samples database.

For the GOSALESDW database in SQL Server and Oracle, type **great_outdoors_warehouse** for the data source name and **GOSALESDW** for the database name. For DB2, type **great_outdoors_warehouse** for the data source name and **GS_DB** for the database name.

The Great Outdoors data source connections appear as entries in the **Data Sources** tab of the **Directory** tool.

You can now import the samples unless there is a syntax error in the connection string or an incorrect parameter.

Set Up Microsoft Analysis Services Cube Samples

Microsoft Analysis Services (MSAS) cubes are provided which you can use from Cognos Connection or Framework Manager. The cube samples are contained in the GOSALESDW.cab and GOSALESDW.abf archive files in the *c8_location*/webcontent/samples/datasources/cubes/MSAS directory. The archive files must be restored to a Microsoft SQL Server database running Microsoft Analysis Services (p. 329).

The Go Sales Fact cube contains the same monthly sales data as the GOSALESDW database.

The GO Finance Fact cube contains year-to-date and monthly financial data for all accounts so you can create model financial statements in Analysis Studio, Query Studio, and Report Studio. The GO Finance Fact cube contains Actuals in US dollars submissions for 2004, 2005, or 2006.

Note: Both Microsoft XML 6.0 Parser and Microsoft SQL 2005 Analysis Services 9.00 OLEDB Provider must be installed on the local client in order to establish data source connections to MSAS cubes.

Steps

1. On the computer where Cognos 8 is installed, go to the *c8_location*/webcontent/samples/datasources/cubes/MSAS/en directory.
2. Copy the GOSALESDW.cab and GOSALESDW.abf files to a directory that you can access from the Analysis Manager console in the Analysis Servers of Microsoft SQL Server.
3. Use the Analysis Manager to restore the database from the GOSALESDW.cab and GOSALESDW.abf files.

You can now create the data source connections using either the GO Sales Fact or GO Finance Fact cubes (p. 333).

Set Up the DB2 Cube Sample

To set up the DB2 cube sample, you must have Hyperion Essbase installed, and a DB2 OLAP Server with Essbase Integration Services Console.

Steps

1. Using Essbase Integration Services Console, perform an outline member load and a data load.

2. Using the GOSLDW_ML database for the cube, import the GOSLDW_EN_FR_DE_JA_RU_SC.xml model and the GOSLDW_*language*.xml metadata outline for the language that you want to use, where *language* is one of: EN (English), DE (German), FR (French), JA (Japanese), RU (Russian) or SC (Chinese).

   Information about cubes is available in the cube details file for each language: DB2OLAPGOSLDW*language*CubeInfo.xml.

3. Using Hyperion Solutions Essbase Administration- Administration Console, set up the generations for the model and populate the cube.

You can now create a data source connection to the cube (p. 333).

Create Data Source Connections to OLAP Data Sources

Cognos 8 provides the following OLAP samples:

- GO Sales Fact and GO Finance Fact Microsoft Analysis Services cubes
- Great Outdoors Company cube
- Great Outdoors DB2 cube

You must create data source connections to the cubes to use the samples. You must set up the Microsoft Analysis Services cube samples or set up the DB2 cube sample, if you are using them, before creating data source connections.

You can increase the read cache size to improve query performance, although this setting has no effect on the initial time required to open a cube.

To create data sources, you must have execute permissions for the Directory secured feature and traverse permissions for the Administration secured function.

Steps for PowerCubes

1. Open Cognos Connection.
2. In the upper-right corner, click **Launch**, **Cognos Administration**.
3. On the **Configuration** tab, click **Data Source Connections**.
4. Click the new data source button.

   Note: You must add a data source connection for each cube.

5. To create a data source connection for the Sales and Marketing cube, type **sales_and_marketing** in the **Name** box, and then click **Next**.

   You can define a Windows path or a UNIX path.

   If you define a UNIX path and you plan to use Framework Manager, you must also define the Windows path and ensure that the cube is also available in the Windows location. Framework Manager can access cubes only from Windows locations.

6. In the connection page, under **Type** click **Cognos PowerCube**, select an isolation level, and then click **Next**.

The connection string page for the selected database appears.

7. In the **Read cache size (MB)** box, type the cache size of the cube in megabytes.

   If you leave this field blank or type 0, Cognos Connection uses the default value in the ppds_cfg.xml file in the configuration folder.

8. In the **Windows location** box, type the location and name of the SalesandMarketing.mdc file for the data source connection. For example, type

   ***c8_location*/webcontent/samples/datasources/cubes/PowerCubes/En/SalesandMarketing.mdc**

9. To test whether the parameters are correct, click **Test**.

10. Click **Finish**.

You can now import the sample package for the PowerCube to use this data source.

Steps for DB2 Cubes

1. Open Framework Manager.

2. Click **Create a new project**.

3. In the **New Project** page, specify a name and location for the project.

4. In the **Select Language** page, click the design language for the project.

5. Click **OK**.

   The Import wizard appears.

6. In the connection page, under **type** click **IBM DB2 OLAP Server**, select an isolation level, and then click **Next**.

   The connection string page for the selected database appears.

7. In the **Server name** box, type the name of the server.

8. To test whether the parameters are correct, click **Test**.

9. Click **Finish**.

To use this data source, you must create a package using this data source in Framework Manager, and then publish the package.

Steps for Microsoft Analysis Service Cubes

1. Open Cognos Connection.

2. In the upper-right corner, click **Launch**, **Cognos Administration**.

3. On the **Configuration** tab, click **Data Source Connections**.

4. Click the new data source button.

5. In the **Name** box, type **go_sales_fact** or **go_finance_fact** and then click **Next**.

6. In the connection page, click the type of Microsoft SQL Server database that you restored and want to connect to, select an isolation level, and then click **Next**.

   The connection string page for the selected database appears.

7. In the **Server Name** box, type the name of the server where the restored databases are located. If needed, in the **Database name** box, type the name of the database you restored.

8. Under **Signons**, select the **Password** and **Create a signon that the Everyone group can use** check boxes, type the user ID and password for the user that you created when you restored the databases, and then click **Finish**.

   Tip: To test whether the parameters are correct, click **Test**.

9. Click **Finish**.

10. You now have the option to create a package using your new data source. Click **Create a Package** and **OK**, and follow the instructions in the new package wizard.

    Note: You must create a package with this data source in order to use this data source, and you must create a connection between the GOSALESDW_MSAS2005.zip deployment and the MSAS service before you can use the samples.

11. Click **New Connection** and follow the steps in the new connection wizard, naming the connection GOSALESDW_MSAS2005, and selecting the database based on the language you are using. For example, GOSALESDW for English, or GOSALESDW_DE for German.

    When the new connection is created, it appears in the data source connection list.

Set Up the Metric Studio Sample

To set up the Metric Studio sample, do the following:

- ❑ Create a metric store named GOMETRICS.
- ❑ Create a new metric package named GO Metrics that uses the GOMETRICS metric store.

  For the data source name, type go_metrics. When prompted by the wizard, select the standard Gregorian calendar and accept the defaults for Years, Quarters, and Months. Select January 1, 2004 as the start date for a period of three years.

  For more information, see the section about metrics in the *Administration and Security Guide*.

- ❑ Set the import source.
- ❑ Import the metric data and files into the metric store.

Steps to Set the Import Source

1. Copy all text files from *c8_location*/webcontent/samples/datasources/metricsdata/*GO_Metrics_Unicode* to *c8_location*/deployment/cmm.

   Tip: You may need to create the cmm folder.

2. Specify the source and collation code for Unicode in Metric Studio.

3. In Metric Studio, in the **Tools** list, click **Import Sources**.
4. Under **Metric Deployment Location**, click **Use the default deployment location**.
5. Click the **Set Properties** icon in the **Actions** column next to the default import source.
6. Under **Character Set Encoding**, select **Unicode (UTF-16)** and click **OK**.

You can now use the GO Metrics package in Metric Studio.

Steps to Import Metric Data and Files into the Metric Store

1. In Metric Studio, in the **Tools** list, click **Import Sources**.
2. Click **New**.
3. In the **Name** box, type a descriptive name for the data source.
4. Click **Metrics import directory**.
5. Specify the identification code. This identifies the new import source.
6. If the folder includes sub-folders, click **Include sub-folders**.
7. In the **File format** box, click **8.3.1**.
8. In the **Character Set Encoding** box, specify **Unicode UTF16** and click **OK**.
9. Choose whether to import the files into the metric store using Cognos Connection or Metric Studio.
   - To use Cognos Connection, in **Public Folders** or **My Folders**, open the GO Metrics package by clicking the view metric package contents icon in the **Actions** column. Click **Metric Maintenance**.
   - To use Metric Studio, in Metric Studio, in the **Tools** list, click **Metric Maintenance**.
10. Click the **Import and transfer data from files into metric store** metric task.

    Tip: If an error occurs, click **Clear staging area rejected data logs**, **Clear metric history data only**, and **Clear metric history and calendar data**.

You can now use the GO Metrics package in Metric Studio.

Import the Samples

To use the sample package and other content, you must import them from the sample deployment archive.

Before you import the Cognos_Samples.zip and GO_Metrics.zip deployment archives, you must restore the databases (p. 329). For each database, you must create one or more named users with select permissions for the database tables. You must also create data source connections to the samples databases (p. 330).

Before you import the Cognos_PowerCube.zip or Cognos_PowerCube_Financial.zip deployment archive, you must create a database connection to the appropriate PowerCube (p. 333) and select the language that you want to use. The language that you select must be supported by your locale.

Steps

1. Copy the zip file from the *c8_location*/webcontent/samples/content directory to the directory where your deployment archives are saved.

   The default location is *c8_location*/deployment. The location is set in the configuration tool. For information about changing the location, see the configuration tool online help.

2. Open Cognos Connection.

3. In the upper-right corner, click **Launch**, **Cognos Administration**.

4. On the **Configuration** tab, click **Content Administration**.

   Note: To access this area in Cognos Administration, you must have the required permissions for the **Administration tasks** secured feature.

5. On the toolbar, click the new import button.

   The **New Import** wizard appears.

6. In the **Deployment Archive** box, select **Cognos_Samples**, **Cognos_Powercubes**, **GO_Metrics**, or **GO_Audit**.

7. Click **Next**.

8. Type a unique name and an optional description and screen tip for the deployment archive, select the folder where you want to save it, and then click **Next**.

9. In the **Public Folders Content** box, select the packages and folders that you want to import.

   The Cognos_Samples deployment archive has the following packages or folders:

   - **GO Data Warehouse (analysis)**, **GO Data Warehouse (query)**, **GO Sales (analysis)**, **GO Sales (query)**, **Sample Template** and **Practical Examples**.

   The Cognos_PowerCube deployment archive for the **Great Outdoors Company** has packages or folders for the following languages:

   - English
   - French
   - German
   - Japanese
   - Russian
   - Simplified Chinese

   The GO_Metrics deployment archive has the following packages or folders:

   - **GO Metrics**

10. Select the options you want, along with your conflict resolution choice for options that you select, and then click **Next**.
11. In the **Specify the general options** page, select whether to include access permissions and references to external namespaces, and who should own the entries after they are imported.
12. Click **Next**.

    The summary information appears.
13. Review the summary information and click **Next**.
14. Select the action that you want:
    - To run once now or later, click **Save and run once**. Click **Finish**, specify the time and date for the run, then click **Run**. Review the run time and click **OK**.
    - To schedule at a recurring time, click **Save and schedule**. Click **Finish**, and then select frequency and start and end dates. Click **OK**.

      Tip: To temporarily disable the schedule, select the **Disable the schedule** check box.
    - To save without scheduling or running, click **Save only** and click **Finish**.
15. When the import is submitted, click **Finish**.

You can now use the sample packages to create reports and analyses in Report Studio, Query Studio, and Analysis Studio, view extracts in Metric Designer, or create agents in Event Studio. You can also run the sample reports that are available on the Public Folders tab in the portal.

Sample Database Models

The following sample models provide information for the fictional company, the Great Outdoors and are provided with Cognos 8:

- go_sales, which refers to the samples database GOSALES
- go_data_warehouse, which refers to the database GOSALESDW
- gosales_scriptplayer, which refers to the samples databases GOSALES

You can use sample database models on different platforms. For information about moving models from one platform to another, see the Framework Manager *User Guide*.

Note: Transformer 8 uses some of the reports in the GO Data warehouse (query) package and GO Sales (query) package as source data for various cubes. These reports are meant to be simple list reports with no formatting. The description information for the reports indicates if the report was developed to be source data for Transformer 8.

GO Sales Model

This model contains sales analysis information for the fictional company, The Great Outdoors. It also has the query items required by the Event Studio samples. The model accesses three schemas and has two packages. One package is based on the dimensional view and the other is baed on the query (relational) view.

GO Data Warehouse Model

This model contains financial, human resources, and sales and marketing information for the fictional company, The Great Outdoors. The model accesses a dimensional relational data source. The model has two packages. One package is based on the dimensional view, the other is based on the query (relational) view.

GO Sales Scriptplayer

These files can be used to run the action logs in sequence. This action generates a model named gosales_scriptplayer, and publishes a package to the content store.

Example - Running the Sample ELM Returns Agent Against Changed Data

You can change data in the GOSALES database if an Event Studio user wants to test the sample agent ELM Returns Agent. The Event Studio user can then run the sample agent twice and detect a new event. For more information, see the Event Studio *User Guide*.

Running the sample agent against changed data involves the following steps:

- The Event Studio user runs the sample agent against the default data and then asks you to change the data.
- You simulate the occurrence of some initial events and then ask the Event Studio user to run the sample agent a second time.
- The Event Studio user runs the sample agent against the changed data. The Event Studio user informs you when the agent has completed running.
- You simulate the passage of time and the resolution of some events and then ask the Event Studio user to run the sample agent a third time.
- The Event Studio user runs the sample agent for the final time. The Event Studio user informs you when the agent has completed running.
- You modify the data so that the ELM Returns Agent detects no events.

Example - Simulate the Occurrence of Initial Events

Run part of the Event_Studio_ELM_Agent_Modify_GOSALES.sql script to simulate the following data changes:

- change the date to the current date
- change the follow-up code to -1 in four records.

  A code of -1 indicates that follow-up is required.

Steps

1. In SQL Query Analyzer, from the **File** menu, click **Open**.
2. Go to *c8_location*/webcontent/samples/datasources/sqlserver and double-click the Event_Studio_ELM_Agent_Modify_GOSALES.sql file.

3. In the toolbar, from the list of databases, click **GOSALES**.
4. In the **Query** window, under **Part 1**, select all sixteen lines of code.
5. From the **Query** menu, click **Execute**.

The database is updated with the changes.

Example - Simulate the Passage of Time and the Resolution of Some Events

Run part of the Event_Studio_ELM_Agent_Modify_GOSALES.sql script to simulate data changes. First, change it so that two days elapsed since the **ELM Returns Agent** sample was last run. Second, for three of the four event instances found the last time that the **ELM Returns Agent** sample ran, change the follow-up code from -1 to +1. This indicates that only one of the these event instances still requires follow-up and the other instances are resolved.

Steps

1. In SQL Query Analyzer, from the **File** menu, click **Open**.
2. Go to *c8_location*/webcontent/samples/datasources/sqlserver and double-click the Event_Studio_ELM_Agent_Modify_GOSALES.sql file.
3. On the toolbar, click **GOSALES** from the list of databases.
4. In the **Query** window, under **Part 2**, select all lines of code that appear after the comments.
5. From the **Query** menu, click **Execute**.

The database is updated with the changes.

Example - Modify the Data So That the ELM Returns Agent Detects No Events

When the Event Studio user finishes running the sample ELM Returns Agent against changed data, they should notify you. You can then modify the GOSALES database so that the agent no longer detects any event instances.

Step

- Run the following sql commands:

  UPDATE GOSALES.RETURNED_ITEM SET FOLLOW_UP_CODE = 0

  UPDATE GOSALES.RETURNED_ITEM SET ASSIGNED_TO = 0

  UPDATE GOSALES.RETURNED_ITEM SET DATE_ADVISED = NULL

The data is modified. The sample ELM Returns Agent is ready to be used by another Event Studio User.

Remove the Samples Databases from Cognos 8

You can delete the packages on which the samples are based after you finish using the sample reports to learn about Cognos 8, including Framework Manager. This action permanently removes the samples from the content store.

Steps

1. Open Cognos Connection.
2. Click the **Public Folders** tab.
3. Select the check box for the sample package you want to delete.
4. Click the delete button on the toolbar, and click **OK**.

   To use the samples again, you must set up the samples.

Chapter 15: Setting Up an Unattended Installation and Configuration

Set up an unattended installation and configuration to

- install an identical configuration across several computers on your network
- automate the installation and configuration process by specifying options and settings for users

Before you set up an unattended installation and configuration, ensure that all the system requirements and prerequisites are met and that all third-party products are installed and configured.

To set up an unattended installation and configuration:

- ❑ configure a transfer specification file (.ats) to specify installation options
- ❑ run the installation tool in silent mode
- ❑ use a preconfigured configuration file from another computer
- ❑ run the configuration tool in silent mode

After you complete these tasks, ensure that the Cognos 8 installation directory on all computers is protected from unauthorized or inappropriate access. Then you will be ready to use Cognos 8.

Set Up an Unattended Installation

Use a transfer specification file (.ats) to copy Cognos 8 components, including Framework Manager or Metric Designer, to your computer without being prompted for information.

By default, each time you install Cognos 8 components using the installation wizard, the options you select are recorded in a transfer specification file. Therefore, if you already installed Cognos 8 components on a sample computer, you can use the generated transfer specification file as a template for unattended installations on different computers.

If you do not use the installation wizard to install components, you can use the default transfer specification file named response.ats that is available on the CD. You must modify the response.ats file for your environment before you can use it for an unattended installation.

You can check if the unattended installation was successful by checking the return status. A value of zero (0) indicates success and all other values indicate that an error occurred.

Steps Using a File Generated by a Previous Installation

1. Use the installation wizard to install Cognos 8 components on your computer.
2. Go to *c8_location*/instlog.

3. Locate the transfer specification file (.ats) that was generated:
   - If you installed Framework Manager, the file name is ts-FRAMEWORK MANAGER-*version-yyyymmdd_hhmm*.ats.
   - If you installed Cognos 8 for reporting, the file name is ts-*Cognos_product-version-yyyymmdd_hhmm*.ats.
   - If you installed Metric Studio, the file name is ts-CMM-*version-yyyymmdd_hhmm*.ats.
   - If you installed Metric Designer, the file name is ts-CMD-*version-yyyymmdd_hhmm*.ats.
4. Copy the transfer specification file to the computer where you plan to install Cognos 8.
5. On the computer where you plan to install the software, insert the appropriate CD and copy the contents of the CD to your computer.
6. Install Cognos 8:
   - On Windows, open a **Command Prompt** window, and change to the win32 directory where you copied the contents of the CD, and then type the following command, where *location* is the directory where you copied *filename*, the transfer specification file:

     issetup -s location/filename.ats
   - On UNIX or Linux, change to the directory where you copied the contents of the CD, and in the directory for your operating system, type the following command, where *location* is where you copied *filename*, the transfer specification file:

     With XWindows, type

     issetup -s location/filename.ats

     Without XWindows, type

     issetupcc -s location/filename.ats

If a return status other than zero (0) is returned, check the log files for error messages. Errors are recorded in the installation directory in the following log file:

- For Framework Manager, the file name is tl-FM-*version-yyyymmdd-hhmm*_summary-error.txt.
- For Cognos 8 reporting server components, the file name is tl-*Cognos_product-version-yyyymmdd-hhmm*_summary-error.txt.
- For Metric Studio components, the file name is tl-CMM-*version-yyyymmdd-hhmm*_summary-error.txt.
- For Metric Designer, the file name is tl-CMD-*version-yyyymmdd-hhmm*_summary-error.txt.

If errors occur before sufficient initialization occurs, log messages are sent to one of the following log files in the Temp directory:

- For Framework Manager, the file name is tl-FM-*version-yyyymmdd-hhmm*.txt.

- For Cognos 8 reporting components, the file name is tl-*Cognos_product-version-yyyymmdd-hhmm*.txt.
- For Metric Studio components, the file name is tl-CMM-*version-yyyymmdd-hhmm*_summary-error.txt.
- For Metric Designer, the file name is tl-CMD-*version-yyyymmdd-hhmm*_summary-error.txt.

Also ensure that the installation directory is protected from unauthorized or inappropriate access.

After all errors are resolved, you can set up an unattended configuration.

Steps Using the Response.ats File

1. On the target computer, insert the CD and copy the contents to your computer.
2. Go to the win32 directory and open the response.ats file in a text editor.

   Each section in the response.ats file corresponds to a dialog box in the installation wizard.
3. Type the installation location of the program files for Cognos 8 in APPDIR=*location*.

   Tip: There should be no space on either side of the equal sign, (=).
4. For the server components of Cognos 8, in the section named [Component List], next to each component:
   - To install the component, type **1**
   - To not install the component, type **0**

   Note: You do not select components for Framework Manager or Metric Designer. All required files are installed.
5. For a Windows installation, for the APPFOLDER= property, type the name of the **Start** menu folder that contains your program shortcuts.

   Tip: To ensure that the shortcut folder is visible to all users, type **1** for the ALLUSERS_FLAG= property.
6. For the install information in the [Install Conditions] section:
   - To specify the condition is true, type **1**
   - To specify the condition is false, type **0**
7. Save the response.ats file to a local directory after you make the necessary changes.
8. Go to the win32 directory.
9. At the command prompt type the following command, where location is the directory where you copied response.ats:
   - On Windows, UNIX with XWindows, and Linux, type

     issetup -s *location*/response.ats
   - On UNIX without XWindows, type

issetupcc -s *location*/response.ats

If a return status other than zero (0) is returned, check the log files for error messages. Errors are recorded in the installation directory in the following log file:

- For Framework Manager, the file name is tl-FM-*version-yyyymmdd-hhmm*_summary-error.txt.
- For Cognos 8 reporting server components, the file name is tl-*Cognos_product-version-yyyymmdd-hhmm*_summary-error.txt.
- For Metric Studio components, the file name is tl-CMM-*version-yyyymmdd-hhmm*_summary-error.txt.
- For Metric Designer, the file name is tl-CMD-*version-yyyymmdd-hhmm*_summary-error.txt.

If errors occur before sufficient initialization occurs, log messages are sent to one of the following log files in the Temp directory:

- For Framework Manager, the file name is tl-FM-*version-yyyymmdd-hhmm*.txt.
- For Cognos 8 reporting components, the file name is tl-*Cognos_product-version-yyyymmdd-hhmm*.txt.
- For Metric Studio components, the file name is tl-CMM-*version-yyyymmdd-hhmm*_summary-error.txt.
- For Metric Designer, the file name is tl-CMD-*version-yyyymmdd-hhmm*_summary-error.txt.

Also ensure that the installation directory is protected from unauthorized or inappropriate access.

After all errors are resolved, you can set up an unattended configuration.

Set Up an Unattended Configuration

Before you set up an unattended configuration, you must export a configuration from another computer that has the same Cognos 8 components installed. You can then run Cognos Configuration in silent mode.

The exported configuration contains the properties of the Cognos 8 components that you installed on the source computer. If you made changes to the global configuration, you must also copy the global configuration file from the source computer to the computer where you plan to run an unattended configuration. Global configuration includes such settings as content locale, product locale, currencies, fonts, and cookie settings. For more information, see "Changing Global Settings" (p. 221).

Ensure that the configuration settings on the local computer are appropriate to use to configure another Cognos 8 computer with the same installed components. For example, if you changed the host name portion of the Gateway URI property from local host to an IP address or computer name, ensure this setting is appropriate for the new computer's configuration.

You can check if the unattended configuration was successful by checking the return status. A value of zero (0) indicates success and all other values indicate that an error occurred.

Steps

1. In Cognos Configuration, from the **File** menu, click **Export as**.
2. If you want to export the current configuration to a different folder, in the **Look in** box, locate and open the folder.

   Ensure that the folder is protected from unauthorized or inappropriate access.
3. In the **File name** box, type a name for the configuration file.
4. Click **Save**.
5. Copy the exported configuration file from the source computer or network location to the *c8_location*/configuration directory on the computer where you plan to do an unattended configuration.
6. Rename the file to cogstartup.xml.
7. If you changed the global configuration on the source computer, copy the coglocale.xml file from the source computer to the *c8_location*/configuration directory on the computer where you plan to do an unattended configuration.
8. Go to *c8_location*/bin.
9. Type the configuration command:
   - On UNIX or Linux, type

     ./cogconfig.sh -s
   - On Windows, type

     cogconfig.bat -s

   Tip: To view log messages that were generated during an unattended configuration, see the cogconfig_response.csv file in the *c8_location*/logs directory.

Cognos Configuration applies the configuration settings specified in the local copy of cogstartup.xml, encrypts credentials, generates digital certificates, and if applicable, starts Cognos 8 service or process.

Chapter 16: Performance Maintenance

This section includes topics about using Cognos and third-party tools and metrics to maintain the performance of your Cognos 8 environment.

System Performance Metrics

Cognos 8 provides system metrics that you can use to monitor the health of the entire system and of each server, dispatcher, and service. You can also set the thresholds for the metric scores. Some examples of system performance metrics are the number of sessions in your system, how long a report is in a queue, how long a Java Virtual Machine (JVM) has been running, and the number of requests and processes in the system.

System performance metrics are available in Cognos Administration, which you can access from Cognos Connection. For more information about using system performance metrics, see the *Administration and Security Guide*.

An added feature is that you can take a snapshot of the current system metrics so that you can track trends over time or review details about the state of the system at a particular time. For more information, see the topic about the metric dump file in the troubleshooting chapter of the *Administration and Security Guide*.

Enabling Only Services That are Required

If some Cognos 8 services are not required in your environment, you can disable them to improve the performance of other services.

For example, to dedicate a computer to running and distributing reports, you can disable the presentation service on a report server computer. When you disable the presentation service, the performance of the report server will improve.

Notes:

- The Presentation service must remain enabled on at least one computer in your Cognos 8 environment.
- If you want to use Query Studio, you must enable the Presentation service.
- If you want to use Analysis Studio, you must enable the Report service.
- If some Cognos 8 components are not installed on a computer, you should disable the services associated with the missing components. Otherwise the Cognos 8 components will randomly fail.

Cognos 8 Services

After you install and configure Cognos 8, one dispatcher is available on each computer by default. Each dispatcher has a set of associated services, listed in the following table.

Service	Purpose
Agent service	Runs agents. If the conditions for an agent are met when the agent runs, the agent service asks the monitor service to run the tasks.
Batch report service	Manages background requests to run reports and provides output on behalf of the monitor service.
Content Manager service	• Performs object manipulation functions in the content store, such as add, query, update, delete, move, and copy • Performs content store management functions, such as import and export
Data movement service	Manages the execution of data movement tasks in Cognos 8. Data movement tasks, such as Builds and JobStreams, are created in Data Manager Designer and published to Cognos 8.
Delivery service	Sends emails to an external SMTP server on behalf of other services, such as the report service, job service, agent service, or data integration service
Event management service	Creates, schedules, and manages event objects that represent reports, jobs, agents, content store maintenance, deployment imports and exports, and metrics
Job service	Runs jobs by signaling the monitor service to run job steps in the background. Steps include reports, other jobs, import, exports, and so on.

Service	Purpose
Log service	Records log messages generated by the dispatcher and other services. The log service can be configured to record log information in a file, a database, a remote log server, Windows Event Viewer, or a UNIX system log. The log information can then be analyzed by customers or by Cognos Customer Support, including: • security events • system and application error information • selected diagnostic information
Metric Studio service	Provides the Metric Studio user interface for monitoring and entering performance information
Migration service	Manages the migration from Cognos Series 7 to Cognos 8.
Monitor service	• Manages the monitoring and execution of tasks that are scheduled, submitted for execution at a later time, or run as a background task • Assigns a target service to handle a scheduled task. For example, the monitor service may ask the batch report service to run a report, the job service to run a job, or the agent service to run an agent. • Creates history objects within the content manager and manages failover and recovery for executing entries
Presentation service	• Transforms generic XML responses from another service into output format, such as HTML or PDF • Provides display, navigation, and administration capabilities in Cognos Connection
Report data service	Manages the transfer of report data between Cognos 8 and applications that consume the data, such as Cognos 8 Go! Office and Cognos 8 Go! Mobile.
Report service	Manages interactive requests to run reports and provides output for a user in Cognos Connection or a studio

Service	Purpose
System service	Defines the Business Intelligence Bus API-compliant service used to obtain application-wide Cognos 8 configuration parameters. It also provides methods that normalize and validate locale strings and map locale strings to locales supported by your application.

Tuning a DB2 Content Store

If you use a DB2 database for the content store (p. 118), you can take steps to improve the speed with which requests are processed.

By default, DB2 assigns tables that contain large objects (LOBS) to a database-managed tablespace. As a result, the LOBS are not managed by the DB2 buffer pools. This results in direct I/O requests on the LOBS, which affects performance. By reassigning the tables that contain LOBS to a system-managed tablespace, you reduce the number of direct I/O requests.

Before changing a DB2 content store, allocate sufficient log space to restructure the database.

To reconfigure the DB2 content store, do the following:

- Export the data from the tables that contain at least one large object (LOB).
- Create the tables in a system-managed table space.
- Import the data into the tables.

Tune Apache Tomcat Settings

If you use Apache Tomcat, you can edit settings to improve performance.

You can edit the maxProcessor and acceptCount settings in the server.xml file.

Steps

1. Open the server.xml file.
2. Edit the settings that appear after the following comment:

   ```
   <!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8080 -->
   ```

   Find the following line:

   ```
   maxProcessors="75"
   ```

   and change it to the following:

   ```
   maxProcessors="1000"
   ```

3. Find the following line:

   ```
   acceptCount="100"
   ```

and change it to the following:

```
acceptCount="500"
```

4. Save the updated server.xml file.

Increase the Request-handling Capacity for Cognos Content Database

Cognos Content Database is configured for use with a small system. If you use Cognos Content Database in a large system, where the number of simultaneous requests is greater than ten, you must adjust the default JVM memory settings and increase the page cache size for Derby.

Steps

1. In the *c8_location*\bin directory, open the derby.sh file.
2. Find the following line:

   ```
   MEM_SETTINGS=-Xmx256m
   ```

   and change it to the following:

   ```
   MEM_SETTINGS="-Xmx1152m -XX:MaxPermSize=128M -XX:MaxNewSize=576m -XX:
   NewSize=288m"
   ```

3. In the *c8_location*\configuration directory, rename derby.properties.sample to derby.properties.
4. In the same directory, open the derby.properties file.
5. Comment out the following line:

   ```
   derby.storage.pageCacheSize=15000
   ```

Improve Metric Store Database Performance

Cognos 8 provides a script called cmm_update_stats that updates your metric store database indexes, which improves performance. Typically, you use this script before or after loading data when the volume or distribution of data has changed significantly. For example, performance may improve if you run this script after increasing the number of scorecards from 100 to 1000.

Steps

1. Ensure that there is no activity in the metric store database.
2. Go to the following directory:

   c8_location\configuration\schemas\cmm
3. Go to the appropriate database directory.
4. Depending on the database type, run one of the following scripts from the command line:

- For Microsoft SQL Server or DB2:

  cmm_update_stats *host_name metric_store_name Admin_user_name password*

- For Oracle:

  cmm_update_stats *metric_store_name Admin_user_name password*

Reduce Delivery Time for Reports in a Network

Reports that are distributed globally take longer to open in remote locations than to open locally. In addition, HTML reports take longer than PDF reports to open because more requests are processed for HTML reports.

You can reduce the amount of time for reports to open in remote locations in two ways. You can reduce the number of requests between the browser and the server by running the report in PDF format. If HTML reports are required, you can speed up the delivery of the report by configuring additional gateways in some of the remote locations. Static content, such as graphics and style sheets, will be delivered faster.

Appendix A: Manually Configuring Cognos 8

The console attached to the UNIX or Linux computer on which you are installing Cognos 8 may not support a Java-based graphical user interface. You must perform the following tasks manually.

- Manually change default configuration settings by editing the cogstartup.xml file, located in the *c8_location*/configuration directory.
- Manually change language or currency support, or locale mapping by editing the coglocale.xml file, located in the *c8_location*/configuration directory.
- Apply the configuration and the locale settings to your computer by starting the Cognos 8 services in silent mode.
- Deploy Cognos 8 into an application server environment by manually creating a Cognos application file.

For all installations, some configuration tasks are required so that Cognos 8 works in your environment. If you distribute Cognos 8 components across several computers, the order in which you configure and start the computers is important.

Other configuration tasks are optional and depend on your reporting environment. You can change the default behavior of Cognos 8 by editing the cogstartup.xml file to change property values. You can also use sample files that enable Cognos 8 to use resources that already exist in your environment.

Manually Configuring Cognos 8 on UNIX and Linux

The console attached to the UNIX or Linux computer on which you are installing Cognos 8 may not support a Java-based graphical user interface. You must

- manually change default configuration settings by editing the cogstartup.xml file, located in the *c8_location*/configuration directory
- manually change language or currency support, or locale mapping by editing the coglocale.xml file, located in the *c8_location*/configuration directory
- apply the configuration and the locale settings to your computer by running Cognos Configuration in silent mode

For all installations, some configuration tasks are required so that Cognos 8 works in your environment. If you distribute Cognos 8 components across several computers, the order in which you configure and start the computers is important.

Other configuration tasks are optional and depend on your reporting environment. You can change the default behavior of Cognos 8 by editing the cogstartup.xml file to change property values. You can also use sample files that enable Cognos 8 to use resources that already exist in your environment.

Manually Change Default Configuration Settings on UNIX and Linux Computers

If the console attached to your UNIX or Linux computer does not support a Java-based graphical user interface, you must edit the cogstartup.xml to configure Cognos 8 to work in your environment.

Note: Some configuration settings are not saved in the cogstartup.xml file unless you use the graphical user interface. For example, the server time zone is not set for your Cognos components when you modify the cogstartup.xml file directly and then run Cognos Configuration in silent mode. In this case, other user settings that rely on the server time zone may not operate as expected.

If you want Cognos 8 to use a resource, such as an authentication provider that already exists in your environment, you can add a component to your configuration. You do this by copying the required XML code from the sample files into the cogstartup.xml file and then edit the values to suit your environment.

Important: By default, the cogstartup.xml file is encoded using UTF-8. When you save the cogstartup.xml file, ensure that you change the encoding of your user locale to match the encoding used. The encoding of your user locale is set by your environment variables.

When you edit the cogstartup.xml file, remember that XML is case-sensitive. Case is important in all uses of text, including element and attribute labels, elements and values.

Before you edit the cogstartup.xml file, ensure that you

- make a backup copy
- create the content store on an available computer in your network
- review the configuration requirements for your installation type

Steps

1. Go to the *c8_location*/configuration directory.
2. Open the cogstartup.xml file in an editor.
3. Find the configuration setting you want to change by looking at the help and description comments that appear before the start tag of the `<crn:parameter>` elements.
4. Change the value of the `<crn:value>` element to suit your environment.
5. Open the cogstartup.xml file in an editor.
6. Find the configuration setting you want to change by looking at the help and description comments that appear before the start tag of the `<crn:parameter>` elements.
7. Change the value of the `<crn:value>` element to suit your environment.

   Tip: Use the `type` attribute to help you determine the data type for the configuration property.
8. Repeat steps 3 to 4 until the configuration values are appropriate your environment.
9. Save and close the file.

You should now use a validating XML editor to validate your changes against the rules in the cogstartup.xsd file, located in the *c8_location*/configuration.

Add a Component to Your Configuration

The cogstartup.xml file contains configuration settings used by Cognos 8 and by default third-party components.You can change the components that Cognos 8 uses by copying XML elements from sample files into the cogstartup.xml file. You can then edit the configuration values to suit your environment.

For example, to use an Oracle database instead of a Microsoft SQL Server database for the content store, you can use the ContentManager_*language code*.xml sample file to replace the default database connection information.

Cognos 8 can use only one instance at a time of the following elements:

- the database for the content store
- a cryptographic provider
- a configuration template for the Cognos 8 service

You should be familiar with the structure of XML files before you start editing them.

Steps

1. Go to the *c8_location*/configuration/samples directory.
2. Choose a sample file to open in an editor:
3. • To use Oracle, DB2, or Sybase for the content store, open the ContentManager_*language_code*.xml file.
4. • To use an authentication provider, open the Authentication_*language_code*.xml file.
5. • To use a third-party cryptographic provider, open the Cryptography_*language_code*.xml file.
6. • To send log messages somewhere other than a file, open the Logging_*language_code*.xml file.
7. • To use a medium or large template for the amount of resources the Cognos 8 process uses, open the CognosService_*language_code*.xml file.
8. Copy the elements that you need.

   Tip: Ensure that you copy the code including the start and end tags for the `<crn:instance>` element.

   For example, look for the (Begin of) and (End of) comments:

```
<!--
================================================
(Begin of) DB2 template
-->
<crn:instance ...>
...
</crn:instance>
<!--
End of) DB2 template
```

```
==========================================
-->
```

9. Go to the *c8_location*/configuration directory.
10. Open the cogstartup.xml file in an editor.
11. Paste the code from the sample file to the cogstartup.xml file and replace the appropriate `<crn:instance>` element.
12. Change the values of these new elements to suit your environment.

    For the `<crn:instance>` element, don't change the class attribute. You can change the name attribute to suit your environment.

    For example, if you use an Oracle database for the content store, change only the name attribute to suit your environment.

    ```
    <crn:instance class="Oracle" name="MyContentStore">
    ```

13. Save and close the file.
14. Run Cognos Configuration in silent mode by typing the following command:

    ./cogconfig.sh -s

    This ensures that the file is valid and that passwords are encrypted.

Manually Change Encrypted Settings

You can manually change encrypted settings, such as passwords and user credentials, in the cogstartup.xml file.

To prompt Cognos Configuration to save an encrypted setting, you change the value and then set the encryption flag to false.

Steps

1. Go to the *c8_location*/configuration directory.
2. Open the cogstartup.xml file in an editor.
3. Find the encrypted setting you want to change by looking at the help and description comments that appear before the start tag of the `<crn:parameter>` elements.
4. Change the value of the `<crn:value>` element to suit your environment.

   Tip: Use the type attribute to help you determine the data type for the configuration property.
5. Change the encryption value to false.

   For example,

   ```
   <crn:value encrypted="false">
   ```

6. Repeat steps 3 to 5 until the configuration values are appropriate for your environment.
7. Save and close the file.

8. Type the following configuration command:

   ./cogconfig.sh -s

The new settings are saved and encrypted.

Manually Change the Global Settings on UNIX and Linux Computers

If the console attached to your UNIX or Linux computer does not support a Java-based graphical user interface, you must manually edit the coglocale.xml file located in the *c8_location*/configuration directory.

You can change global settings

- to specify the language used in the user interface when the language in the user's locale is not available
- to specify the locale used in reports when the user's locale is not available
- to add currency or locale support to report data and metadata
- to add language support to the user interface

By default, Cognos 8 components ensure that all locales, which may come from different sources and in various formats, use a normalized form. That means that all expanded locales conform to a language and regional code setting.

Before you can add language support to the user interface, you must install the language files on all computers in your distributed installation. For more information, contact your Cognos support representative.

Example 1

A report is available in Content Manager in two locales, such as en-us (English-United States) and fr-fr (French-France), but the user locale is set to fr-ca (French-Canadian). Cognos 8 uses the locale mapping to determine which report the user sees.

First, Cognos 8 checks to see if the report is available in Content Manager in the user's locale. If it is not available in the user's locale, Cognos 8 maps the user's locale to a normalized locale configured on the Content Locale Mapping tab. Because the user's locale is fr-ca, it is mapped to fr. Cognos 8 uses the mapped value to see if the report is available in fr. In this case, the report is available in en-us and fr-fr, not fr.

Next, Cognos 8 maps each of the available reports to a normalized locale. Therefore, en-us becomes en and fr-fr becomes fr.

Because both report and the user locale maps to fr, the user having the user locale fr-ca will see the report saved with the locale fr-fr.

Example 2

The user's locale and the report locales all map to the same language. Cognos 8 chooses which locale to use. For example, if a user's locale is en-ca (English-Canada) and the reports are available

in en-us (English-United States) and en-gb (English-United Kingdom), Cognos 8 maps each locale to en. The user will see the report in the locale setting that Cognos 8 chooses.

Example 3

The report and the user locales do not map to a common language. Cognos 8 chooses the language. In this case, you may want to configure a mapping. For example, if a report is available in en-us (English-United States) and fr-fr (French-France), but the user locale is es-es (Spanish-Spain), Cognos 8 chooses the language.

Steps

1. On every computer where you installed Content Manager, go to the *c8_location*/configuration directory.
2. Open the coglocale.xml file in an editor.
3. Add or modify the required element and attribute between the appropriate start and end tags.

Type of element	Start tag	End tag
Language	<supportedProductLocales>	</supportedProductLocales>
Content Locales	<supportedContentLocales>	</supportedContentLocales>
Currency	<supportedCurrencies>	</supportedCurrencies>
Product Locale Mapping	<productLocaleMap>	</productLocaleMap>
Content Locale Mapping	<contentLocaleMap>	</contentLocaleMap>
Fonts	<supportedFonts>	</supportedFonts>

Tip: To remove support, delete the element.

4. Save and close the file.

Tip: We recommend that you use a validating XML editor to validate your changes against the rules in the cogstartup.xsd file, located in the *c8_location*/configuration.

If you add a currency code that is not supported by Cognos, you must manually add it to the i18n_res.xml file in the *c8_location*/bin/ directory. Copy this file to each Cognos computer in your installation.

Starting and Stopping Cognos 8 in Silent Mode on UNIX and Linux Computers

You run Cognos Configuration in silent mode to apply the configuration settings and start the services on UNIX or Linux computers that do not support a Java-based graphical user interface.

Before you run the configuration tool in silent mode, you should ensure the cogstartup.xml file is valid according to the rules defined in the cogstartup.xsd file. The cogstartup.xsd file is located in the *c8_location*/configuration directory.

Steps to Start Cognos 8

1. Ensure that the cogstartup.xml file, located in the *c8_location*/configuration directory, has been modified for your environment.

   For more information, see "Manually Change Default Configuration Settings on UNIX and Linux Computers" (p. 356).

2. Go to the *c8_location*/bin directory.

3. Type the following command

   ./cogconfig.sh -s

   Tip: To view log messages that were generated during an unattended configuration, see the cogconfig_response.csv file in the *c8_location*/logs directory.

Cognos Configuration applies the configuration settings specified in the cogstartup.xml file, encrypts credentials, generates digital certificates, and if applicable, starts the Cognos 8 service or process.

Steps to Stop Cognos 8

1. Go to the *c8_location*/bin directory.

2. Type the following command

   ./cogconfig.sh -stop

Manually Create a Cognos Application File

Cognos 8 and the servlet gateway must be packaged into an application file for deployment to supported third-party application servers (p. 301), (p. 233). Cognos 8 provides a Build Application wizard that you can use to create the application file.

You can create a Web archive (.war) file, an Enterprise archive (.ear) file, or an expanded directory that includes all the files necessary for the application. For information about WAR and EAR files or expanded directories and to determine what is supported by your application server, see the documentation provided with the application server.

If you choose not to use the Build Application wizard, you must complete the following steps to create the application file.

If the application server is not being used as a web server, you do not need to include the Cognos static content (html pages, images, and so on) in the application file. Excluding the static content when creating the application file reduces the size of the file.

Steps to Create a Cognos 8 Application File

1. Go to the *c8_location*/war/p2pd directory.

2. Run the build script by using the following command syntax:

   - For Windows,

     build.bat ***file_type option***

   - For UNIX or Linux,

     build.sh ***file_type option***

   where *file_type* can be one of the following:

Value	Description
war	WAR file with static content
war_without_webcontent	WAR file with no static content
war_without_docsamples	WAR file with static content and with no documentation and sample files
ear	EAR file with static content
ear_without_webcontent	EAR file with no static content
ear_without_docsamples	EAR file with static content and with no documentation and sample files
expand	directory containing the application with static content
expand_without_webcontent	directory containing the application with no static content
expand_without_docsamples	directory containing the application with static content and with no documentation and sample files

   and where *option* can be one or more of the following:

Option	Value	Description
-Dappserver_type=*value*	jboss other (default)	Perform actions for a JBoss application server Perform actions for a non-JBoss application server

Option	Value	Description
-Dcontext_root=*value*	p2pd (default)	Preset a context root value for the application
-Dwar_name=*value*	*path/filename* Default is ../../p2pd.war	Path and name of the WAR file to be created
-Dear_name=*value*	*path/filename* Default is ../../p2pd.ear	Path and name of the EAR file to be created
-Dexpand_location=*value* (For expand file types)	*path/directory* Default is ../../temp/expand	Path to directory where the application files are to be expanded

Steps to Create a Servlet Gateway Application File

1. Go to the *c8_location*/war/gateway directory.
2. Run the build script by using the following command syntax:
   - For Windows,

     build.bat ***file_type option***
   - For UNIX or Linux,

     build.sh ***file_type option***

   where *file_type* can be one of the following:

Value	Description
gateway_war	WAR file with static content
gateway_war_without_docsamples	WAR file with static content and with no documentation and sample files
gateway_ear	EAR file with static content
gateway_ear_without_docsamples	EAR file with static content and with no documentation and sample files
expand	directory containing the application with static content

Value	Description
expand_without_docsamples	directory containing the application with static content and with no documentation and sample files

and where *option* can be one or more of the following:

Option	Value	Description
-Dappserver_type=*value*	jboss other (default)	Perform actions for a JBoss application server Perform actions for a non-JBoss application server
-Dcontext_root=*value*	ServletGateway (default)	Preset a context root value for the application
-Dwar_name=*value*	*path/filename* Default is ../../ServletGateway.war	Path and name of the WAR file to be created
-Dear_name=*value*	*path/filename* Default is ../../ServletGateway.ear	Path and name of the EAR file to be created
-Dexpand_location=*value*	*path/directory* Default is ../../temp/expand	Path to directory where the application files are to be expanded

Appendix B: Troubleshooting

Use this troubleshooting reference information and solutions as a resource to help you solve specific problems you may encounter during or after the installation of Cognos 8 components.

For more information about troubleshooting resources, see the Troubleshooting section of the *Adminsitration and Security Guide*.

Problems are characterized by their symptoms. Each symptom can be traced to one or more causes by using specific troubleshooting tools and techniques. After being identified, each problem can be fixed by implementing a series of actions.

When you are troubleshooting, log files can help you. Another valuable troubleshooting tool is the Knowledge Base, which is available on the Cognos support site (http://support.cognos.com). The Knowledge Base is a database of problems and solutions for all Cognos products.

When you cannot resolve a problem, the final resource is your Cognos technical support representative. To analyze a problem, your technical support representative requires information about the situation and the symptoms that you are experiencing. To help isolate the problem, collect the necessary data before you contact your representative.

Log Files

Log files can help you troubleshoot problems by recording the activities that take place when you work with a product. Operations performed in Cognos 8 are recorded in various log files for tracking purposes. For example, if you experienced problems installing Cognos 8, consult the transfer log file to learn what activities the installation wizard performed while transferring files.

Before you begin viewing log files, ensure that they contain the information that you need. The number of log files and the information they contain are set by parameters in Cognos Connection and in Cognos Configuration.

Use Cognos Administration in Cognos Connection to learn about logging categories and how to set the level of detail to log for each category.

For more information, see the Cognos 8 *Administration and Security Guide*.

Use Cognos Configuration to specify the size, number, and location of log files, and to configure the properties of the log server. For more information, see the Cognos Configuration *User Guide*.

When troubleshooting, the following files can assist you:

The Transfer Log File

This file records the activities that the installation wizard performed while transferring files. The transfer log file is located in the *c8_location*\instlog directory. The file name identifies the product name, version, and build number, and includes a time stamp. The following is an example of the file name format:

tl-C8BISRVR-8.1-0.0-20050901_1122.txt

The Transfer Summary-Error Log File

This file records the components you installed, disk space information, the selections you made in the transfer dialogs, and any errors the installation wizard encountered while transferring components. The transfer summary-error log file is located in the *c8_location*/instlog directory. The file name identifies the product name, version, and build number, and includes a time stamp. The following is an example of the file name format:

tl-C8BISRVR-8.1-0.0-20050901_1122_summary_error.txt

The Startup Configuration File

This file records your configuration choices each time you save your property settings. The file name is cogstartup.xml. If you are unable to save your configuration, or are having problems you can revert to a previously saved configuration file. The backup configuration files are located in the *c8_location*/configuration directory. The following is an example of the file name format for backup configuration files:

cogstartup_200211231540.xml

The Startup Configuration Lock File

This file is created each time you open Cognos Configuration. It prevents you from opening more than one Cognos Configuration window. If you experience problems opening Cognos Configuration, you can check the *c8_location*/configuration directory for the cogstartup.lock file. If the file exists and Cognos Configuration is not open, it means that Cognos Configuration did not shut down properly the last time you used it. You can delete the lock file and then open Cognos Configuration.

The Locale Configuration File

This file records the configuration choices you make in Cognos Configuration for product and content locales, locale mapping, and currency support. If you experience problems with language support in the user interface or in reports, use these files to track your changes. The backup configuration files are located in the *c8_location*/configuration directory. The following is an example of the file name format:

coglocale_200211231540.xml

The Run-Time Log File

The default Cognos log file named cogserver.log file, or other log files that you configure to receive log messages from the log server, record information after you start the Cognos 8 service. They are located in the *c8_location*/logs directory. If you configured another destination for log messages, check the appropriate file or database.

Some log messages indicate problems. Most messages provide information only, but others can help you to diagnose problems in your run-time environment.

The Gateway Log File

The gateways record errors in the gateway log file, which is located in the *c8_location*/logs directory. You can use the gateway log file to troubleshoot problems that prevent the gateway from processing requests or from using encryption. Symptoms of these problems are user IDs and passwords do not work, single signon does not work, and the dispatcher is running but users receive the following error message: `The Cognos BI server is not available`. The gateway log file uses the following naming format, where *gateway_interface* is cgi, mod (Apache 1.3 module), mod2 (Apache 2.0 module), or isapi.

gw*gateway_interface*.log (e.g., gwcgi.log)

The Uninstallation Log File

This file records the activities that the Uninstall wizard performed while uninstalling files. The log file is named cognos_uninst_log.htm and is located in the Temp directory. You can use the log file to troubleshoot problems related to uninstalling Cognos 8 components.

The Silent Mode Log File

This file records the activities that Cognos Configuration performed while running in silent mode. This log file is named cogconfig_response.csv and is located in the *c8_location*/logs directory.

The ReportNet(R) to Cognos 8 Upgrade File

This file contains a summary of the results of an upgrade from ReportNet to Cognos 8. The log file is named upgradeLog.xml and is located in the *c8_location*/logs directory. The file is in xml format and references an xslt style sheet. You can double-click the file to have it appear in your browser.

Problems Starting Cognos 8

You may encounter problems when you try

- to start the Cognos 8 service
- to open the Welcome page for Cognos Connection for the first time
- to start an application server, such as WebLogic or WebSphere

Symptoms	Solution
You do not see the splash screen for Cognos Connection when you start Cognos 8.	Check your Web server configuration.
The service starts but no tables are created in the content store database.	Check your content store configuration.

Symptoms	Solution
The service does not start.	Ensure that you wait a few moments before submitting a request.
The third-party application server does not start.	Check the file permissions and directory names of the application server installation location.

Ensure that you use third-party software that is supported by Cognos components. You can view an up-to-date list of environments, such as operating systems, patches, browsers, Web servers, directory servers, and database servers on the Cognos Global Customer Services Web site (http://support.cognos.com).

CFG-ERR-0106 Error When Starting the Cognos 8 Service in Cognos Configuration

When you start the Cognos 8 service, you may receive the following error message:

CFG-ERR-0106 Cognos Configuration received no response from the Cognos 8 service in the allotted time. Check that Cognos 8 service is available and properly configured.

There are two possible causes for this problem:

- The Cognos 8 service needs more time to start.
- A standby Content Manager computer may be configured incorrectly.

The Cognos 8 Service Needs More Time

By default, Cognos Configuration checks the progress of the start request every half second for three minutes. If Cognos Configuration does not receive a response within this time, the error message appears.

To avoid this error, you can change the amount of time that Cognos Configuration waits to receive a response from the Cognos 8 service. You do this by configuring the ServiceWaitInterval and ServiceMaxTries properties in the *c8_location*/configuration/cogconfig.prefs file.

The ServiceWaitInterval property represents the time interval, in milliseconds, at which Cognos Configuration checks the progress of the start request. By default, its value is 500, which is equivalent to half a second.

The ServiceMaxTries property represents the number of times that Cognos Configuration checks the progress of the start request. By default, its value is 360.

Content Manager Is Configured Incorrectly

If the error message appears on a standby Content Manager computer, the setting for storing the symmetric keys may be incorrect.

To avoid this problem, configure the standby Content Manager computer to store the symmetric keys locally.

Steps to Change the Wait Time

1. Using Cognos Configuration, stop the Cognos 8 service.
2. Open the *c8_location*/configuration/cogconfig.prefs file in an editor.

   This file is created automatically the first time you open Cognos Configuration.
3. Add the following code to the file:

   ServiceWaitInterval=*number of milliseconds*

   ServiceMaxTries=*number of times*

   Tip: Add the numeric values that correspond to your configuration needs.
4. Save the file.
5. Using Cognos Configuration, start the Cognos 8 service.

Steps to Store Symmetric Keys Locally

1. On the standby Content Manager computer, start Cognos Configuration.
2. In the **Explorer** window, under **Security**, click **Cryptography**.
3. In the **Properties** window, under **CSK settings**, set **Store symmetric key locally** to **True**.
4. From the **File** menu, click **Save**.
5. From the **Actions** menu, click **Start**.

   This action starts all installed services that are not running. If you want to start a particular service, select the service node in the **Explorer** window and then click **Start** from the **Actions** menu.

Unable to Start the Cognos 8 Service Because the Port is Used by Another Process

You may not be able to start the Cognos 8 service or process if one of the default ports is used by another process.

Tip: To view the current network TCP/IP network connections, use the netstat command.

Use Cognos Configuration to change the default port that Cognos 8 uses.

When you change the port used by the local dispatcher, you must change the value of the Dispatcher URI properties. Because the change affects all the URIs that are based on the local dispatcher, you must change the URIs of all local components. By default, local components contain localhost in the URI.

For example, if you install all components on one computer and you want to change the dispatcher port, replace 9300 in all dispatcher and Content Manager URIs with the new port number.

Steps to Change the Default Port

1. Start Cognos Configuration.
2. In the **Explorer** window, click the appropriate group or component:
   - To access the port number in the dispatcher and Content Manager URIs, click **Environment**.
   - To access the port number for the local log server, under **Environment**, click **Logging**.
   - To access the shutdown port number, under **Environment**, click **Cognos 8 service**, **Cognos 8**.
   - To access the port number for the location of the applications.xml file used by Portal Services, under **Environment**, click **Portal Services**.
3. In the **Properties** window, click the **Value** box next to the property that you want to change.
4. Change the value from 9300 to the new value.

   Ensure that you change the ports in all URIs that contain localhost:9300.
5. From the **File** menu, click **Save**.
6. From the **Action** menu, click **Start**.

Cognos 8 Service Does Not Start or Fails After Starting

You start the Cognos 8 service but services either do not start correctly or are very slow to start. After services start, the system fails a short time afterwards. While services are starting, Java uses 100 percent of the CPU time. You may also receive multiple occurrences of error messages such as the following:

- *DPR-DPR-1035 Dispatcher detected an error.*
- *CAM-CRP-1157 Unable to synchronize the local common symmetric key store with Content Manager.*

If you use a DB2 database for the content store, ensure that the database version and Java version are compatible. For DB2 version 8.2, Java 1.5 is not supported. For DB2 version 9, Java 1.5 is supported on all operating systems except HPUX and Solaris.

To review an up-to-date list of environments supported by Cognos products, such as operating systems, patches, browsers, Web servers, directory servers, database servers, and application servers, visit the Cognos Global Customer Services Web site (http://support.cognos.com).

546816

Cognos 8 Server Fails to Start and Gives No Error Message

A Cognos 8 server may fail to start after an upgrade or new installation, but no error message appears. This may occur when a previously running or new Cognos 8 server is configured to use a large amount of memory.

If the server on which Cognos 8 is installed contains version 1.0 of Microsoft security update 921883, there may be an issue when a lot of contiguous memory is requested by an application.

This is a known issue with version 1.0 of Microsoft security patch 921883. Microsoft distributed a second version of the patch to fix the problem. As a workaround, uninstall the first security patch, or install version 2.0 of the patch. Alternatively, you can configure the Cognos 8 server to use less memory.

For more information, see the Microsoft knowledge base article about programs using a lot of contiguous memory failing, at http://support.microsoft.com.

Cognos BI Server Not Available When Starting Cognos 8

After you configure Cognos components and start the Cognos 8 services, when you open Cognos Connection, the following error message may appear:

The Cognos Gateway is unable to connect to the Cognos BI server.

The server may be unavailable, or the gateway may not be correctly configured.

Check the Cognos server log file for more information. By default, the cogserver.log file is located in the *c8_location*/logs directory. If you configured another destination for log messages, check the appropriate file or database.

Content Manager may not be able to connect to the content store if the content store is not configured properly. This may occur if

- the content store uses an unsupported character encoding
- the content store uses a database collation sequence that is case sensitive
- the configuration settings you specified in Cognos Configuration are not valid

Unsupported Character Encoding

If the following messages appear in the log file, the database you created for the content store does not use a supported character encoding:

- For Oracle:

  CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

  CM-SYS-5121 Content Manager cannot start because the database character set for the content store is not supported.

  CM-SYS-5126 The content store database server uses the character set US7ASCII.

  CM-SYS-5125 The content store database client uses the character set US7ASCII.

- For DB2 UDB:

  CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

  CM-SYS-5121 Content Manager cannot start because the database character set for the content store is not supported.

  CM-SYS-5124 The content store database server uses the code page 1252.

- For Sybase:

  CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

  CM-SYS-5121 Content Manager cannot start because the database character set for the content store is not supported.

For Content Manager to connect to the content store, the content store must use the appropriate character encoding.

Database	Character encoding
Oracle 9i	AL32UTF8 AL32UTF16
DB2 UDB	Codeset UTF-8
Sybase ASE	UTF-8
Microsoft SQL Server	UTF8 UTF16

To resolve this problem, you must recreate the content store database using the correct character encoding, or convert the character encoding. For more information, see the database vendor documentation.

Case Sensitive Collation Sequence

If the following messages appear in the log file, the database you created for the content store uses a database collation sequence that is case sensitive:

CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

CM-SYS-5122 The content store database has a default collation that is case-sensitive. Content Manager requires a content store that has a case-insensitive collation.

CM-SYS-5123 The content store database server uses the collation <parameter>.

CM-SYS-5007 Content Manager build @cm_build_version@ failed to start! Review the Content Manager log files and then contact your system administrator or customer support.

To resolve this problem, you must recreate the content store database using a database collation sequence that is not case sensitive. For more information, see the database vendor documentation.

Invalid Configuration Settings

If the following or similar messages appear in the log file, you did not configure the content store correctly in Cognos Configuration.

- For Microsoft SQL Server:

  CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

  CM-CFG-5036 Content Manager failed to connect to the content store. The connection string is "jdbc:JSQLConnect://localhost:1433/cm".

  Failed Logon:com.jnetdirect.jsql.x: Cannot open database requested in login 'cm'. Login fails. url:jdbc:JSQLConnect://localhost:1433/cm.

- For DB2:

  CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

  CM-SYS-5003 Content Manager is unable to access the content store. Verify your database connection parameters and then contact your database administrator.

  [IBM][CLI Driver] SQL1013N The database alias name or database name "CM123" could not be found.

- For Oracle:

  CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

  CM-CFG-5036 Content Manager failed to connect to the content store. The connection string is "jdbc:oracle:thin:@localhost:1521:pb1".

  ORA-01017: invalid username/password; logon denied.

- For Sybase:

  CM-CFG-5063 A Content Manager configuration error was detected while connecting to the content store.

  CM-CFG-5036 Content Manager failed to connect to the content store. The connection string is "jdbc:sybase:Tds:localhost:5000/cm".

  JZ006: Caught IOException: java.net.ConnectException: Connection refused: connect.

If you are using an Oracle database, do not use illegal characters such as an underscore in Cognos Configuration for the Service Name property. If the Service Name includes illegal characters, tables are not created in the content store database when the Cognos 8 service is started.

Steps for Microsoft SQL Server, Oracle, DB2, and Sybase

1. On the computer where you installed Content Manager, start Cognos Configuration.

2. In the **Explorer** window, under **Data Access**, **Content Manager**, right-click **Content Store** and click **Delete**.

   This deletes the default resource. Content Manager must be configured to access only one content store.

3. Right-click **Content Manager**, and then click **New resource**, **Database**.

4. In the **Name** box, type a name for the resource.

5. In the **Type** box, select the type of database and click **OK**.

   If you are upgrading and want to use an existing content store, ensure that you select the type of database you use for the older version of ReportNet.

   If you installed more than one version of Cognos 8, you must use a different content store for each version. When a content store is used by a new version of Cognos 8, it cannot be used by an older version of ReportNet.

   Tip: If you want to use Oracle Net8 keyword-value pair to manage the database connection, select **Oracle database (Advanced)**.

6. In the **Properties** window, provide values depending on your database type:

   - If you use a Microsoft SQL Server database, type the appropriate values for the **Database server with port number or instance name** and **Database name** properties.

     For a Microsoft SQL Server database, you can choose to use a port number, such as 1433, or a named instance as the value for the **Database server with port number or instance name** property.

     To connect to a named instance, you must specify the instance name as a JDBC URL property or a data source property. For example, you can type **localhost\instance1**. If no instance name property is specified, a connection to the default instance is created.

     Note that the properties specified for the named instance, along with the user ID and password, and database name, are used to create a JDBC URL. Here is an example:

     jdbc:JSQLConnect://localhost\\instance1/user=sa/*more properties as required*

   - If you use a DB2 database, for the **Database name** property, type the database alias.

   - If you use an Oracle database, type the appropriate values for the **Database server and port number** and **Service name** properties.

   - If you use an advanced Oracle database, for the **Database specifier** property, type the Oracle Net8 keyword-value pair for the connection.

     Here is an example:

     (description=(address=(host=myhost)(protocol=tcp)(port=1521)(connect_data=(sid=(orcl)))))

   - If you use a Sybase database, type the appropriate values for the **Database server and port number** and **Database name** properties.

7. If you want to change the logon credentials, specify a user ID and password:

- Click the **Value** box next to the **User ID and password** property and then click the edit button when it appears.
- Type the appropriate values and click **OK**.

8. From the **File** menu, click **Save**.

   The logon credentials are immediately encrypted.

9. Test the connection between Content Manager and the content store.

   Tip: In the **Explorer** window, right-click the new database and click **Test**.

   Content Manager connects to the database, checks the database permissions, and creates and populates a table. The table is not deleted and is used each time that the test is repeated.

Cannot Log On to a Namespace When Using Cognos Connection (PRS-CSE-1255 Error)

You open Cognos 8 through Cognos Connection. However, when you attempt to create a data source and log on to a namespace, the following error messages appear:

- *PRS-CSE-1255 Exception error encountered in data decryption*.
- *CAM-CRP-1064 Unable to process the PKCS #7 data because of an internal error. Reason: java.lang.IndexOutOfBoundsException*.

This issue may occur if you do not have the necessary permissions for the following directories:

- c8\configuration
- c8\configuration\csk
- c8\configuration\encryptkeypair
- c8\configuration\signkeypair

The solution is to enable the read and execute permissions on the directories listed above for anyone who must start the Cognos 8 service.

Cognos 8 Services Fail to Restart After a Network Outage

The Cognos Bootstrap Service restarts Cognos 8 services after a network outage for Tomcat installations where a network IP address is specified in the internal dispatcher URI. During the restart, The Cognos 8 services may not initialize successfully, requiring a manual restart after the network is restored.

To resolve the problem, configure the **Internal dispatcher URI** property in Cognos Configuration to use localhost or the network host name.

No Warning That Installing a Later Version of Cognos 8 Will Automatically Update the Earlier Version of the Content Store

You have a version of ReportNet installed on your computer. You install a later version into a new location. You use the same database for the content store for both versions. After you configure the later version and start the Cognos 8 service, the earlier version of ReportNet no longer works because all content is automatically upgraded.

If you want to use different versions of ReportNet and Cognos 8 after you upgrade, ensure that before you install the later version, you

- back up the database you use for the content store
- restore the backup to a new location

Alternatively, you can choose to use the deployment tool to import the entire content store from an earlier version to the later version. All existing content in the content store database is replaced by the imported content. You receive a warning message about this.

Download of Resource Fails

You start Report Studio in Internet Explorer and the following error message appears:

The download of the specified resource has failed.

This problem may be caused by recent Microsoft XMLHTTP upgrades if you do not have a language preference set in Internet Explorer.

To resolve the problem, specify a language preference in Internet Explorer.

DB2 Returns SQL1224N Error When Connecting from AIX

If your content store is a DB2 database and you receive an SQL1224N error on AIX, check the db2diag.log file for additional information about the error.

If the error includes reason code 18, you may need to change the DB2 configuration to accept more connections. For more information, see the IBM DB2 support pages for the error SQL1224N.

Content Manager Error When Starting Cognos 8

After starting Cognos 8, no BIBUSTKSERVMA process is started. There are errors listed in the pogo******.log and cogserver.log files. Users receive errors in the browser when connecting to Cognos Connection.

In the pogo******.log file, an error related to Content Manager appears.

In the cogserver.log file, the following error appears:

An attempt to register the dispatcher in Content Manager was unsuccessful. Will retry periodically.

When connecting to http://*computer name*/cognos8, the following error messages appear in the browser:

- *DPR-ERR-2058 The dispatcher cannot service the request at this time. The dispatcher is still initializing*
- *SoapSocketException: Connection Refused*

Cognos Configuration uses a user ID to bind to the LDAP database. If this user ID is moved to another group, Cognos Configuration can no longer locate it.

To correct the problem, move the user ID back to the original group.

Cannot Open an MS Cube or PowerCube

You are unable to open an MS Cube or PowerCube, or you can open an MS Cube but only metadata is shown. For an MS Cube, you may receive the following error message:

MO-ERR-0030

"Cannot connect to the datasource. Please set the service to run as a domain user with the correct privileges."

To solve this problem, ensure that the user running the Cognos 8 service has access rights to the cube.

PowerCubes are accessed through mapped drives or UNC path names.

Steps for MS Cubes

1. Add the domain user account that starts the Cognos 8 service to the **Act as part of the operating system** privilege:
   - Under Administrative Tools, select **Local Security Policy**.
   - Expand **Security Settings**, **Local Policies** and click **User Rights Assignment**.
   - Right-click the **Act as part of the operating system** policy and select **Properties**.
   - Click **Add User or Group** and add the user account that starts the Cognos 8 service.
2. If you use the domain userID and password method of authentication, add the user account that starts the Cognos 8 service to the domain that includes Content Manager, the report server (Application Tier Components), IIS Web server, and the data source server (Microsoft SQL Server or Microsoft Analysis Server).
3. If you use an external namespace, such as Active Directory Server, for authentication, add the user account that starts the Cognos 8 service to the domain that includes the authentication provider.

   This domain must also include Content Manager, the report server (Application Tier Components), IIS Web server, and the data source server (Microsoft SQL Server or Microsoft Analysis Server).

For more information about configuring external namespaces for authentication, see the topics about authentication providers in the *Installation and Configuration Guide*.

Step for PowerCubes

- Ensure that the Cognos user profile has sufficient operating system or domain access rights to open the PowerCube file.

  For information, see the *Administration and Security Guide*.

Cannot Open an OLAP Data Source

You cannot open one of the following data sources:

- MSAS
- Essbase
- DB2

You can try opening the same cube with Excel. This will tell you whether the OLAP server is configured and running, and whether the appropriate client software is installed.

The Page Cannot Be Found When Starting Cognos 8 in Windows 2003

After installing Cognos 8 on Windows 2003, the following message may appear when you try to start Cognos 8:

The page cannot be found. The page you are looking for might have been removed, had its name changed, or is temporarily unavailable. HTTP Error 404 - File or Directory not found.

This error is caused by a security feature in Windows 2003 Internet Information Services (IIS). This security feature does not allow unknown cgi file extensions.

To resolve this problem, add a new file extension in IIS for the cognos.cgi file. For more information, see the IIS documentation.

The Page Is Not Shown When Opening a Portal After Installing Cognos 8

After you install and configure Cognos 8, you are unable to open Cognos Connection.

This may be because the Web server is not properly configured. For example, the virtual directories required for Cognos 8 may not exist or they may point to the wrong physical folders.

For information about configuring the Web server, see the *Installation and Configuration Guide*.

DPR-ERR-2058 Error Appears in Web Browser When Starting Cognos 8

After you start the services in Cognos Configuration and then try to open the portal, a message similar to one of the following may appear:

DPR-ERR-2058 The dispatcher encountered an error while servicing a request. XTS handler must be initialized before being invoked.

DPR-ERR-2058 The dispatcher cannot service the request at this time. The dispatcher is still initializing. Please try again or contact your administrator.

These error messages usually occur when the dispatcher cannot communicate with Content Manager. To help you determine the specific cause, look in the cogserver.log file in the *c8_location*/logs directory. The most common causes are listed below, with solutions.

Cognos Services are Not Done Initializing

After you start the services in Cognos Configuration and the configuration tool shows that the services are running, wait a few minutes for all services to start before you open the portal.

Content Manager is Not Available

In a distributed installation, ensure that Content Manager is installed, configured, and running. Ensure also that the other Cognos computers are configured with the correct Content Manager URI.

The Content Store is Not Available or is Not Configured Properly

Ensure that the content store database was created and that you configured it correctly in Cognos Configuration.

Tables are Not Created in the Content Store

Ensure that you are using a version of DB2, Microsoft SQL Server, Oracle, or Sybase that is supported by Cognos components.

The Logon Credentials for the Content Store Are Incorrect

Check whether the information changed. For example, DB2 reads information from the NT user management. If the password for the NT account changed, you must also change the logon credentials for the content store in Cognos Configuration.

Check for special characters in the logon password. Occasionally, the JDBC driver does not accept characters that are reserved for xml, such as %, !, <, and >.

The User Does not Have Appropriate Permissions

Ensure that the user has the appropriate permissions.

Out of Memory on HP-UX

If you are using Tomcat, you can determine the issue is related to HP-UX server configuration. You may be exceeding the expected maximum number of simultaneously active threads per process.

Steps to Check for an HP-UX Configuration Problem

1. In the /bin/startup.sh file, find

   ../tomcat4.1.27/bin/catalina.sh start "$@"

2. Change it to the following:

../tomcat4.1.27/bin/catalina.sh run "$@"

The run command causes the Tomcat output to appear in the console window for Cognos 8.

3. Stop and restart Cognos 8 using the ./shutdown.sh and ./startup.sh commands.

   If the following error message appears in the console window for any of the application servers, the issue is an HP-UX configuration problem:

   OutofMemoryException error: Unable to create new native thread on HP-UX.

   The problem is that the default values for HP-UX 11.0 and 11i are set too low for most Java applications.

   Tip: You can check the number of threads in your process by using the -eprof option available in JDK 1.1.8 and by analyzing the Java.eprof file using HPjmeter by selecting the threads metric.

Steps to Increase the maximum Number of Threads Per Process

1. Have your system administrator change the Kernel parameter as follows:
   - max_thread_proc = 512
   - nkthread = 1024
2. Ensure that the ulimit settings are unlimited.

Content Manager Cannot Connect to the Content Store on Oracle

If you are using an Oracle database as a content store, the DPR-ERR-2058 error may be generated when logging onto the portal http://host_name/cognos8. All tables are created on the database.

You may also receive the following error messages:

- *CM-CFG-5036 Content Manager failed to connect to the content store.*
- *ORA-01017: invalid username/password; logon denied*

Steps to Set the Oracle Database Server Name

1. In the **Explorer** window, click **Data Access**, **Content Manager**, **Content Store**.
2. Change the Oracle database server name to a fully qualified name such as host_name.companyname:1534 to match the name in the tnsnames.ora file.

EBA-090034 Error When Starting WebLogic 8

After configuring WebLogic 8 to use SSL, you used the command startManagedWebLogic.cmd to start the application server. The application server did not start and you received the following error message:

EBA-0990034 Not listening for SSL

The problem occurred because WebLogic 8 has a feature that is incompatible with the Cognos 8 bcprov-jdk14.134.jar file.

To resolve the problem, you must add a new version of the BouncyCastle bcprov .jar file to the WebLogic Java extension directory.

Steps

1. From the BouncyCastle Web site, http://www.bouncycastle.org/download/, download a compatible BouncyCastle bcprov .jar file, such as bcprov-jdk14-137.jar.
2. Copy the downloaded .jar file to the WebLogic Java extension directory, *WebLogic_location*\jdk142_*nn*\jre\lib\ext.
3. In the *WebLogic_location*\jdk142_*nn*\jre\lib\security directory, edit the java.security file and add the following line to the provider list:

   ```
   security.provider.6=org.bouncycastle.jce.provider.BouncyCastleProvider
   ```

Report Studio Does Not Start

You may not be able to start Report Studio if you are using pop-up blocking software on your computer.

When you start Report Studio, it opens in a new browser window. In addition, a new browser window opens when you run a report and when an error is detected.

To correct the problem, disable any pop-up blocking software when working in Report Studio.

DPR-ERR-2022 Error Appears in Web Browser When Starting Cognos 8

After you start the services in Cognos Configuration and then try to open the portal, a message similar to the following may appear:

DPR-ERR-2022 No response generated. This may be due to an incorrect configuration, a damaged installation, or the dispatcher not having finished initializing.

Opening the Portal Too Soon

This problem can occur if you try to open the portal before Cognos services are initialized.

To avoid this problem, after you start the services in Cognos Configuration and the configuration tool shows that the services are running, wait a few minutes for all services to start before you open the portal.

The system.xml File Contains Errors

The system.xml file may have been edited.

Replace the system.xml file in the *c8_location*\templates\ps\portal directory with a copy from backup or use an XML editor to edit it.

Unable to Download the cognos.xts File

After installing Cognos 8, you are prompted to download the cognos.xts file when opening Cognos Connection. The following error message may appear:

You have chosen to download a file from this location. cognos.xts from servername

This problem occurs when the permissions on the virtual directories are not set properly. You must provide the cgi-bin virtual directory in the Microsoft Internet Information Service (IIS) with execute permissions.

To resolve this problem, recreate the virtual directories in IIS with the following permissions.

Alias	Path	Permissions
cognos8	*c8_location*\Program Files\ Cognos\c8\webcontent	Read
cognos8\ cgi-bin	*c8_location*\Program Files\ Cognos\c8\cgi-bin	Read Execute
cognos8\help	*c8_location*\Program Files\ Cognos\c8\webcontent\ documentation	Read

Application Server Startup Script Fails

You may have problems running the startup scripts for an application server to deploy the Cognos application if Cognos 8 components are installed in a directory with a name that includes spaces.

To resolve this problem, rename the directory and do not include spaces in the new name. If this solution is not easily handled by the startup scripts, try adding quotation marks around the directory name that includes spaces or use the 8.3 naming convention.

Deploying Cognos 8 to an Oracle Application Server or IBM WebSphere Application Server Fails

Deploying Cognos 8 to an Oracle application server or an IBM WebSphere application server may fail with any of the following errors:

- Browser timeout in administration console
- Error Message: HTTP 500 Internal Error
- Error Message: Deployment failed: Base Exception: java.rmi.RemoteException (Oracle)
- Return to application file selection page (IBM WebSphere)

These errors can occur because the application file that you are trying to deploy is too large.

To solve this problem, do the following:

- If you are using the **Build Application Wizard**, clear the **Include static files from the Webcontent folder** check box when you select the application to build.

This will reduce the size of the application file. If static content is required, you can manually copy it to the deployed application location after you have successfully deployed Cognos 8 into the application server.

- If you are deploying the application file manually for an Oracle application server, type the following command:

  dcmctl deployapplication -f ***path_and_name_of_ear_file*** **-a** ***application_name*** **-co** ***OC4J_instance_name***

  This command is not supported for Oracle Release 3.

For more information about deploying Cognos 8 to an application server, see the *Installation and Configuration Guide*.

Microsoft Excel 2000 Multipage Report Type Does Not Work

To ensure that report URLs cannot be changed when passed from a client browser to the report server, Cognos 8 applies signatures to the URLs it generates. However, Excel 2000 multipage (XLS) does not support signed URLs. To use the Excel 2000 multipage report type, you must disable digital signing of the URLs by doing the following:

Steps to Disable Signed URLs

1. Stop the dispatcher.
2. In the *c8_location*/configuration directory, rename the cafconfig.xml.sample file to cafconfig.xml.
3. Open the cafconfig.xml and find the following section:

```
<!--Should we reject unsigned requests for /gd/ urls.
(e.g. multipage excel reports)
Default: true-->
<crn:parameter name="caf_signedReportUrls">
<crn:value xsi:type="xsd:boolean">true</crn:value>
</crn:parameter>
```

4. Change `="xsd:boolean">true</crn:value>` to `="xsd:boolean">false</crn:value>`.
5. Restart your dispatcher.
6. Repeat the above steps for every dispatcher in your environment, or copy the cafconfig.xml to each *c8_location*/configuration directory and restart the dispatchers.

Unable to Deserialize Context Attribute Error When Deploying the p2pd.war File to WebLogic

When you deploy the p2pd.war file to WebLogic, you may see the following error:

Error [context]Could not deserialize context attribute

java.io.NotSerializableException: com.cognos.logserver.LogService

This error does not affect the deployment of the p2pd.war file.

To avoid this problem, add at least one language preference in Internet Explorer.

Error Appears After Upgrading Cognos 8 on a WebLogic Application Server

You are using WebLogic and upgrade Cognos 8 from an earlier release. After you deploy the p2pd.war file for the new installation, a message similar to the following may appear:

<BEA-101215> <Malformed Request "null". Request parsing failed, Code: -10>

This can occur if you undeploy Cognos 8 from WebLogic and some files from the earlier version are not removed from the system.

To solve this problem, use the administrative tools for your application server to ensure that Cognos 8 has been undeployed. For information about undeploying applications, see your application server documentation.

If the directory to which Cognos 8 was originally deployed is not removed during the undeploy process, delete the directory. Also, remove any Cognos 8 .jar files that are cached in your application server environment. For example, in WebLogic 7.0, .jar files are sometimes left in %WL_HOME%\user_projects\<*domain-name*>\<*managed-server-name*>\.wlnotdelete\c8_p2pd_p2pd\jarfiles

You can remove them by deleting the WEB-INF directory.

In WebLogic 8.1.2, the cache location is %WL_HOME%\user_projects\domains\<*domain-name*>\<*managed-server-name*>\.wlnotdelete\extract\c8_p2pd_p2pd\jarfiles

After you remove all files from the previous installation, you can redeploy Cognos 8.

Chinese, Japanese, or Korean Characters Are Different After Upgrade

If you use Chinese, Japanese, or Korean characters, you may notice differences in some characters after upgrading to Cognos 8.

Examples

- You run an existing report. When you compare the output to the same report in ReportNet, you see that some of the characters are different.
- You do a search that you did in ReportNet and get different results.

The differences occurred because the conversion tables that are used for Chinese, Japanese, and Korean were modified to meet global standards. If your report specifications or search filters contain expressions that use constant values, the results may be affected.

If you want to use the same conversion table that you used in ReportNet, run the following script in the *c8_location*/bin directory:

- On UNIX, type

  conv_compat.sh

- On Linux, type

  conv_compat.sh

- On Windows, type

conv_compat.cdm

Accented or Double-Byte Characters May Not Display Correctly When Installing Cognos 8 on Linux

If you are using issetup under a UTF-8 locale, accented or double-byte characters may not display correctly.

To resolve this problem when installing in German or French, use a non-UTF-8 locale and then launch issetup or use the character-mode program issetupcc to install Cognos 8.

To resolve this problem when installing in Japanese, use the character-mode program issetupcc and change the encoding setting of X Terminal to Shift-JIS, then install Cognos 8.

Problems Configuring Cognos 8

After you install Cognos 8 components, you may encounter problems when you save changes in Cognos Configuration.

Ensure that you

- configure and start the services on the computer where Content Manager is located before you configure other components
- restart the Cognos 8 service after you make any configuration changes

Run Database Cleanup Scripts

In some troubleshooting situations, you may be advised to start with new configuration data.

You can run an SQL script to delete all the tables in any of the following databases that Cognos 8 components use:

- content store for data that Cognos 8 needs to operate
- delivery database for report notifications
- log database for log messages
- metric store for metric package content and Metric Studio user preferences

When you delete a table, its structural definition and data are deleted permanently from the database. For the metric store, database objects may also be deleted.

When you restart the Cognos 8 service, a new set of required database tables are created automatically in the location specified by your configuration settings.

Steps

1. On each computer where Content Manager is located, stop the Cognos 8 service.
2. Go to the appropriate directory:

- To delete tables from the log database, go to *c8_location*\configuration\schemas\logging.
- To delete tables from the content store, go to *c8_location*\configuration\schemas\content.
- To delete tables from the notification database, go to *c8_location*\configuration\schemas\delivery.
- To delete tables from the metric store, go to *c8_location*\configuration\schemas\cmm.

3. Go to the appropriate database directory.
4. Depending on the database and database type, run one of the following scripts in the appropriate database tool to delete the tables.

Database	Database Type	Script Name
Content store	DB2	dbClean_db2.sql
	Derby	dbClean_derby.sql
	Microsoft SQL Server	dbClean_mssqlserver.sql
	Oracle	dbClean_oracle.sql
	Sybase	dbClean_sybase.sql
Notification	DB2	NC_DROP_DB2.sql
	Derby	NC_DROP_Derby.sql
	Microsoft SQL Server	NC_DROP_MS.sql
	Oracle	NC_DROP_ORA.sql
	Sybase	NC_DROP_SYBASE.sql
Log	DB2	LS_dbClean_db2.sql
	Derby	LS_dbClean_derby.sql
	Microsoft SQL Server	LS_dbClean_mssql.sql
	Oracle	LS_dbClean_oracle.sql
	Sybase	LS_dbClean_sybase.sql

Database	Database Type	Script Name
Metric store	DB2	cmm_purge_deleted_data *dbalias username password* Specify the dbalias only if a database with the same name is already cataloged.
	Microsoft SQL	cmm_purge_deleted_data *metric_store_name database_name Admin_user_name password*
	Oracle	cmm_purge_deleted_data *database_name database_user_name password* Replace *database_name* with the name in the tnsnames.ora file that refers to the database SID for Metric Studio

5. Start the Cognos 8 service.

Error Trying to Encrypt Information When Saving Your Configuration

When you save your configuration using the configuration tool, you may see an error message that the cryptographic information cannot be encrypted. An error occurred when requesting a certificate from the Certificate Authority.

The cryptographic information cannot be encrypted. Do you want to save the configuration in plain text?

Before you can encrypt your configuration settings, the computer where Content Manager is installed must be configured and running. On UNIX, ensure that you copied the appropriate .jar files to the installation location of your Java Runtime Environment. In addition, ensure that your Java environment is configured correctly, the URIs are correct, and the same certificate authority password is configured for all Content Manager computers.

On Linux, ensure that you copied the appropriate .jar files to the installation location of your Java Runtime Environment.

Also, an error message similar to the following may appear:

java.lang.NoClassDefFoundError: javax/net/ServerSocketFactory.

The cryptographic error usually means the Java environment is not configured correctly. Ensure that the JAVA_HOME environment variable is set correctly and the appropriate security providers are installed, such as JSSE for JRE 1.31.

Steps to Check the Configuration

1. On the Content Manager computer, start Cognos Configuration.
2. In the **Explorer** window, click **Environment**.
3. In the **Properties** window, verify these properties:
   - Under **Gateway Settings**, **Gateway URI**
   - Under **Dispatcher Settings**, **External dispatcher URI** and **Internal dispatcher URI**
   - Under **Other URI Settings**, **Dispatcher URI for external applications** and **Content Manager URIs**
4. In the **Explorer** window, click **Security**, **Cryptography**, **Cognos**.
5. In the **Properties** window, under **Certificate Authority settings**, click the value for **Password**.

   Ensure that the same password is used on all Content Manager computers.
6. Save the configuration and restart Cognos 8.

Problems Generating Cryptographic Keys in Cognos Configuration

When you uninstall Cognos 8, some temporary folders are left behind. Reinstalling the product to the same location without first removing the temporary folders may cause problems while attempting to generate the cryptographic keys in Cognos Configuration.

To resolve this problem, uninstall Cognos 8, remove the *c8_location*/temp/cam folder, and install Cognos 8 again.

CAM-CRP-1315 Error When Saving Configuration

When you save your configuration, you may receive the following error message:

CAM-CRP-1315 Current configuration points to a different Trust Domain than originally configured.

This error occurs when there has been a change to your environment's trust domain. The trust domain is managed by the Certificate Authority associated with the content store. This error can occur if the content store you originally used has been removed or if you modified your configuration to use a Content Manager associated with a different content store after you have saved your original configuration.

To resolve the problem, change your configuration to use the original content store or regenerate the cryptographic keys.

Steps to Regenerate Cryptographic Keys

1. On the Content Manager computer, back up the existing cryptographic keys by saving the following directories to an alternate location that is secure:
   - *c8_location*/configuration/csk
   - *c8_location*/configuration/encryptkeypair
   - *c8_location*/configuration/signkeypair
2. Delete the csk, encryptkeypair, and signkeypair directories.
3. In Cognos Configuration, save the configuration and restart the services.
4. Repeat steps 1 to 3 on all computers that have Cognos 8 components installed.

Configuration Data is Locked by Another Instance of Cognos Configuration

You may get an error message that the configuration data is locked by another instance of Cognos Configuration.

When you start Cognos Configuration, it checks to see if the cogstartup.lock file exists in *c8_location*/configuration. The file may exist if a previous instance did not shut down properly or if another instance of Cognos Configuration is running.

If another instance of Cognos Configuration is running, you should exit that instance. Otherwise, any changes you make to the local configuration may result in errors.

If no other instance of Cognos Configuration is running, delete the cogstartup.lock file in *c8_location*/configuration.

If the Cognos8 service is stopped, click **Start**.

Unable to Exit a Tab Sequence When Using Keyboard-only Navigation in Cognos Configuration

If you use the Tab key to navigate in Cognos Configuration, you may experience problems exiting a tab sequence. For example, in the Properties window, you can press the Tab key to move from one property to another.

However, because Cognos Configuration is a Java application, when you want to close the Properties window, you must press Ctrl+Tab.

Unable to Save Your Configuration

You may be unable to save your configuration because you are missing a resource. For example, you delete a resource such as the Cognos namespace, a cryptographic provider, or the content store. You can replace the default database type for the content store with Oracle, DB2, or Sybase. You

cannot replace the Cognos namespace. You can recreate it, but you must then recreate your Cognos groups and roles.

For more information about creating groups and roles in Cognos Connection, see the *Administration and Security Guide*.

Steps to Recreate the Cognos Namespace

1. Start Cognos Configuration.
2. In the **Explorer** window, under **Security**, right-click **Authentication** and then click **New resource**, **Namespace**.
3. In the **Name** box, type a name for the resource.
4. In the **Type** box, click **Cognos**, and then click **OK**.

   The Cognos namespace appears in the **Explorer** window.
5. From the **File** menu, click **Save**.

Java Error When Starting Cognos Configuration

When you start Cognos Configuration, you may receive an error message that the Java Runtime Environment (JRE) has changed and that the current cryptographic information is not compatible with the new JRE. You may then be prompted to regenerate the cryptographic information for the new JRE or exit to switch back to the previous JRE.

This error may occur for one of these reasons:

- Your configuration data was encrypted using a different JRE than the one Cognos 8 components are currently using.
- The cryptographic information may have been corrupted.

If you click **Regenerate** in the error dialog, the Cognos 8 service is stopped and the cryptographic information is regenerated.

If you click **Exit** in the error dialog, you must set the JAVA_HOME environment variable to point to the JRE that you used to save your configuration.

On Windows, if you want Cognos 8 components to use the JRE that is installed by default, unset JAVA_HOME or set JAVA_HOME to *c8_location*/bin/jre.

Note: If you want to change from one JRE to another, see the topic on changing the version of JVM that Cognos 8 components use. For more information, see the *Installation and Configuration Guide*.

Cryptographic Error When Starting Cognos Configuration

When you start Cognos Configuration, the following error message may appear:

The cryptographic information may have been corrupted or the cogstartup.xml file is invalid. You may have to fix this file or remove it from disk. For more information, see the Installation and Configuration Guide.

This error occurs when Cognos 8 components detect an error in the cogstartup.xml file. This can occur when the cogstartup.xml file is manually edited and there is an error in the changed text.

To resolve the problem, replace the cogstartup.xml file with a copy from your backup location.

Current Configuration Settings Are Not Applied to Your Computer

You change default property values or add a resource to your installation in Cognos Configuration. After saving the current configuration, you may not see the changes or be able to use the resource in the run-time environment.

To apply the new settings to your computer, you must restart the Cognos 8 service.

Steps to Restart the Cognos 8 Service

1. Start Cognos Configuration.
2. From the **Actions** menu, click the appropriate command:
   - If the Cognos 8 service is currently running, click **Restart**.

     This action starts all installed services that are not running and restarts services that are running. If you want to restart a particular service, select the service node in the **Explorer** window and then click **Restart** from the **Actions** menu.
   - If the Cognos 8 service is stopped, click **Start**.

     This action starts all installed services that are not running. If you want to start a particular service, select the service node in the **Explorer** window and then click **Start** from the **Actions** menu.

CM-CFG-029 Error When Trying to Save a Configuration That Specifies a SQL Server Data Source

In Cognos Configuration, you try to save a configuration and the following error message appears in the cogserver.log file:

CM-CFG-029 Content Manager is unable to determine whether the content store is initialized.

EXECUTE permission is denied on object "sp_tables", database "master", owner "dbo'.

This indicates that you do not have the correct permissions to initialize a content store or create a table in the database.

The solution is to ensure that the content store user has permissions to use the sp_tables stored procedure in the master database.

Users are Prompted for Active Directory Credentials

The single signon mechanism does not work when Cognos 8 is configured as follows:

- Microsoft Internet Explorer runs on a Windows NT computer.
- The authentication namespace is configured with the Active Directory provider.

- Microsoft Internet Explorer on a Windows 2000 or Windows 2003 server is configured for Integrated Windows Authentication.

As a result, users are prompted for their Active Directory credentials.

This problem occurs because the Cognos 8 Active Directory provider uses ADSI protocol and Kerberos delegation for authentication in a single signon environment. When Microsoft Internet Explorer runs on Windows NT, it cannot authenticate to the IIS server using Kerberos delegation.

When your system is configured for Windows Integrated Authentication, for the single signon to work with IIS, you must

- configure Cognos 8 to communicate with the Active Directory server using the LDAP provider.
- configure the external identity mapping property to read the REMOTE_USER environment variable.

Font on UNIX Not Found When Starting Cognos Configuration

When you start Cognos Configuration, the following error message may appear:

Font specified in font.properties not found...

This is a common problem on UNIX. It means that the Java Virtual Machine (JVM) is trying to use one or more fonts that are not installed on your computer. However, the JVM should use the system default, and Cognos Configuration should start and run normally.

To avoid these errors, add the missing fonts to your Java Runtime Environment by editing the font.properties files. Several font.properties files, which contain standard font environment information, are installed with your Java SDK. You can find these files in the *JRE_location*/lib directory.

For more information, see the Java documentation.

Unable to Load DB2 OLAP Library in Framework Manager

You installed the DB2 OLAP 8.1 client and cannot load the DB2 OLAP library into Framework Manager. You receive the following message:

DB2-ERR-0028 Unable to load the following DB2 OLAP library: "C:\ibm\db2olap\bin\essapin.dll"

Cognos 8 is configured to use the DB2 OLAP library for Version 8.2. To resolve this problem, you must edit the qfs_config.xml file and rename the library for Version 8.1.

Steps

1. In the *c8_location*\configuration directory, edit the qfs_config.xml file.
2. Find the following code:

   ```
   <provider name="DB2OlapODP" libraryName="doodp82" connectionCode="DO"/>
   ```

3. Change the library name from doodp82 to doodp81 and save the changes.

Group Membership is Missing From Active Directory Namespace

If an Active Directory namespace is configured for the same forest and a user is authenticated using a credential, the group membership will be missing.

The process identity of Cognos 8, when running as a local system account or a domain user, must have one of these privileges:

- impersonate a client after authentication
- act as part of the operating system

If the privilege is missing, there is no group membership for the authenticated user.

To solve this problem, perform the following steps.

Steps

1. From the **Start** menu, click **Settings**, **Control Panel**.
2. Click **Administrative Tools**, and then double-click **Local Security Policy**.
3. In the console tree, click **Security Settings**, **Local Policies**.
4. Click **User Rights Assignment**.
5. Add the process identity of Cognos 8 to one of the following policies:
   - Impersonate a client after authentication

     The default is Administrators, Service.

     For more information, see http://technet2.microsoft.com/WindowsServer/en/Library/fe1fb475-4bc8-484b-9828-a096262b54ca1033.mspx
   - Act as part of the operating system

     The default is Local system.

     For more information, see http://technet2.microsoft.com/WindowsServer/en/Library/ec4fd2bf-8f91-4122-8968-2213f96a95dc1033.mspx

   Both of these privileges give an account the ability to act as another user.

   The privilege Impersonate a client after authentication is similar to the Act as part of the operating system privilege except that it will only allow a process to impersonate after authentication, whereas the privilege Act as part of the operating system allows a process to impersonate before authentication.

   For more information, see http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/tkerbdel.mspx

Deploying Cognos 8 to an Oracle Application Server or IBM WebSphere Application Server

You are deploying Cognos 8 to an Oracle application server or an IBM WebSphere application server and you receive the following errors:

- *Browser timeout in administration console*
- *Error Message: HTTP 500 Internal Error*
- *Error Message: Deployment failed: Base Exception: java.rmi.RemoteException* (Oracle)
- *Return to application file selection page* (IBM WebSphere)

This error can occur because the application file that you are trying to deploy is too large.

To solve this problem, on an Oracle application server, you can deploy the application file manually using the following command:

dcmctl deployapplication -f <*path and name of ear file*> -a <*application name*> -co <*OC4J instance name*>

For either IBM WebSphere or Oracle application servers, clear the **Include static files from the Webcontent folder** option when you use the **Build Application Wizard**. Not including the static content will reduce the size of the application file. If static content is required, you can manually copy it to the deployed application location after you have successfully deployed Cognos 8 into the application server.For more information about deploying Cognos 8 to an application server, see the *Installation and Configuration Guide*.

Errors Displayed Deploying to Oracle 10G Application Server

You are deploying Cognos 8 to an Oracle 10G Application Server, and get the following error messages:

CMM-APP-3254 The initialization of the metrics store failed. DIS-ERR-3115 Task execution failed.

MDS-RUN-3213 Unable to locate database bulk load utility. Please install the appropriate database tool for this platform ('bcp' for SQL Server, 'sqlldr' for Oracle)

This occurs because the bulk loading utilities (SQL Loader on Oracle) are not included in the deployment file created by Cognos Configuration.

To resolve this error, you must use the Oracle client software on the computer where you installed the Oracle 10G Application Server to install the missing components. Ensure that you install SQL Loader.

Page Cannot be Found Error Running Reports using Cognos 8 Go! Office

In a Microsoft Office document configured for Cognos 8 Go! Office, you use Run Report but receive a "The page cannot be found" error message.

This can occur if the Cognos 8 gateway and dispatcher use "localhost" as the server name values on the Cognos 8 server.

To correct this, use the computer name for the gateway and dispatcher host values instead of "localhost".

Error Initializing Oracle Content Store After Upgrade from ReportNet

You are creating a content store in Oracle or upgrading a ReportNet content store in Oracle to Cognos 8, and you receive the following error message:

Content Manager can not initialise the content store with the assistance of the initialisation file: dbupgrade2_0021-to-2_0022_oracle.sql ORA-22858 invalid alteration of datatype

This error occurs if the Oracle database compatibility level is set lower than 9.0.1.

You can correct this by changing the compatibility level to 9.0.1 or higher and restarting the Oracle instance.

CGI Timeout Error While Connected to Cognos 8 Components Through a Web Browser

When performing operations through your Web browser, you receive the following error message:

CGI Timeout, process will be deleted from server.

The error occurs when you use Windows Internet Information Services (IIS) as your Web server and the gateway is configured to use CGI. IIS has a default timeout for CGI applications.

To resolve this problem, you can configure the gateway to use ISAPI. IIS does not have a default timeout for ISAPI applications. Or, if you want to keep using a CGI gateway, you can increase the CGI timeout in IIS.

Steps to Change the Gateway to ISAPI

1. On the gateway computer, start Cognos Configuration.
2. Under **Environment**, for the **Gateway URI** property, change the cognos.cgi portion of the URI to

   cognosisapi.dll
3. In your Web browser, specify the ISAPI URI:

   http://*computer_name*/cognos8/isapi

Steps to Increase the CGI Timeout

1. In the Windows administrative tools, open Internet Information Services.
2. Under the local computer node, right-click **Websites** and select **Properties**.
3. In the **Home Directory** tab, click **Configuration**.
4. In the **Process Options** tab, increase the CGI script timeout.

Servlet Class Fails to Load in WebLogic

You may have problems when configuring a distributed server installation and using WebLogic as the application server for Cognos 8.

When deploying the p2pd.war for the Application Tier Components computer, you may receive servlet exceptions and the dispatcher does not start. The cogserver.log is also not created.

The following error messages appear in the WebLogic Server console:

<Jul 9, 2004 3:47:37 PM EDT> <Error> <HTTP><BEA-101249> <[ServletContext (id=19023494,name=p2pd,context-path=/p2pd)]:Servlet class com.cognos.pogo.isolation. ServletWrapper for servletcfgss could not be loaded because the requested class was not found in the classpath /host2/bea812/user_projects/domains/c8/applications/p2pd/WEB-INF/classes. java. lang.ClassNotFoundException: com.cognos.pogo.isolation.ServletWrapper.>

<Jul 9, 2004 3:47:37 PM EDT> <Error> <HTTP> <BEA-101216> <Servlet: "cfgss" failed to preload on startup in Web application: "p2pd".

javax.servlet.ServletException: [HTTP:101249][ServletContext (id=19023494,name=p2pd,context-path=/p2pd)]: Servlet class com.cognos.pogo.isolation. ServletWrapperfor servlet cfgss could not be loaded because the requested class was not found in the classpath /host2/bea812/user_projects/domains/c8/applications/p2pd/WEB-INF/classes.java. lang.ClassNotFoundException: com.cognos.pogo.isolation.ServletWrapper. at weblogic.servlet. internal.ServletStubImpl.prepareServlet (ServletStubImpl.java:799)

at weblogic.servlet.internal.WebAppServletContext.preload Servlet(WebAppServletContext.java: 3252)

To avoid this problem, do not deploy the p2pd application from the WebLogic applications directory. Create the p2pd directory in another location and deploy p2pd from there.

Steps

1. Open Cognos Configuration and configure the Application Tier Components computer.
2. Restart the Content Manager computer.
3. Create a p2pd directory in a location that is accessible by the WebLogic server but is not in the WebLogic applications directory.

   For example, create a directory named p2pd in the following location:

   WebLogic_location/user_projects/*domain_name*
4. Create the p2pd.war file.
5. In the p2pd directory, extract the p2pd.war file to the WebLogic installation using the following command:

   %JAVA_HOME%/bin/jar xvfm "c8_location/p2pd.war" .
6. Start WebLogic.
7. In the WebLogic Server Console, deploy the p2pd application.

Desktop Icons or Cognos Configuration Window Flicker on Windows

When you run Cognos Configuration on Windows, you may notice that the desktop icons or the Cognos Configuration window flickers.

To resolve this issue, start Cognos Configuration using the -noddraw command line option.

Glossary

access permissions

Rules defining the access rights to resources. Access permissions can be granted to any combination of namespaces, groups, or users. Examples of resources are reports and folders.

alias

In modeling and database terminology, a secondary name for a database table. Aliases are used to create a distinct reference to the table in the model, so that self-joins can be created or ambiguous query paths can be resolved.

In map information technology, a secondary name for a map feature. Aliases are used to create a reference between custom map feature names and feature names in databases.

anonymous access

A method of accessing resources in which users are not authenticated, and all users gain the same access permissions.

application tier components

For installation, the processors that access the query databases to gather information and then render the results as PDF and HTML reports and metrics. Application tier components also pass requests to Content Manager and render the results that Content Manager retrieves from the content store.

authentication

The process of verifying the identity of users when they log on. Users must be authenticated before they can be authorized to use any secured resources.

authentication provider

The communication mechanism to an external authentication source. Functionality such as user authentication, group membership, and namespace searches are made available through authentication providers.

certificate

A document that identifies someone or something by name. Certificates are issued by certification authorities. Each Cognos computer in a distributed installation uses a different certificate. Certificates are used to positively identify an entity. They are used for digital signatures and secure communications, and can be used for encryption or decryption.

certification authority

Certification authority (CA) is the Cognos component that issues certificates identification) to each computer on which components are installed. You can also use a third-party certificate authority.

cipher suite

In SSL, a set of authentication, encryption, and data integrity algorithms used for exchanging messages between network nodes. During an SSL handshake, the two nodes negotiate to see which cipher suite to use when transmitting messages back and forth.

common gateway interface

(CGI) A standard that describes how Web servers should access other programs to create a document that will appear in a Web browser. For example, Web servers often use CGI programs to process forms.

connection

The named information that defines the type of the data source, its physical location, and any signon requirements. A data source can have more than one connection.

content locale

A code that is used to set the language or dialect used for browsers, report text, and so on; and the regional preferences, such as formats for time, date, money, money expressions, and time of day.

For Cognos products, you can specify a locale for the product interface (product locale) and for the data in the report (content locale).

Content Manager

The Cognos 8 service that manages the storage of customer applications, including application-specific security, configuration data, models, metrics, reports, and report output. Content Manager is needed to publish models, retrieve or store report specifications, manage scheduling information, and manage the Cognos namespace.

content store

The database that contains data that Cognos 8 needs to operate, such as report specifications, published models, and the packages that contain them; connection information for data sources; information about the external namespace, and the Cognos namespace itself; and information about scheduling and bursting reports.

Design models and log files are not stored in the content store.

The Cognos 8 service that uses the content store is named Content Manager.

credentials

Information stored about the identity of a Cognos user, usually a user name and password. You can assign your credentials to someone else so that they can use resources that you are authorized to use.

Credentials are created for Cognos components. If a user schedules or programs an action, credentials must be stored in the content store.

data source

A relational database, dimensional cube, file, or other physical data store that can be accessed though Cognos 8.

deployment archive

A file used for deployment. A deployment archive contains the data from the content store that is being moved.

gateway

An extension of a Web server program that transfers information from the Web server to another server. Gateways are often CGI programs, but may follow other standards such as ISAPI and Apache Modules.

glyph

An image of a character in a font.

Letters are glyphs, but in most cases, the term is used in discussions of non-alphabetic writing systems.

group

In security, a list of users or other groups that can be used to assign access permissions and capabilities.

Groups can be referenced from third-party authentication sources or can be local to Cognos 8. Local groups are managed from the administration portal. The list of groups that an authentication user is a member of is part of the user's passport for a Cognos 8 session.

In reporting, grouping is the action of organizing common values of query item together and only displaying the value once. Headers and footers often appear after each instance of a common value in a grouped column

HTTPS

A secure version of HTTP Hypertext Transfer Protocol that incorporates secure sockets layer (SSL)
.

Cognos products use HTTPS and SSL to encrypt and transmit passwords securely over the Internet.

job

A group of runnable objects, such as reports, agents, and other jobs that you run and schedule as a batch.

job step

The smallest part of a job that can be run separately. Usually, a job step is a report. A job step can also be another job.

locale

A code that is used to set the language or dialect used for browsers, report text, and so on; and the regional preferences, such as formats for time, date, money, and money expressions.

For Cognos products, you can specify a locale for the product interface (product locale) and for the data in the report (content locale).

metric package

A Cognos Connection representation of a Metric Studio application. A metric package contains connection information, reports, and metric management tasks for that application.

metric store

A database that contains content for metric packages. A metric store also contains Metric Studio settings, such as user preferences.

namespace

For authentication and access control, a configured instance of an authentication provider. Allows access to user and group information.

In XML, a collection of names, identified by a URI reference, which are used in XML documents as element types and attribute names.

In Framework Manager, namespaces uniquely identify query items, query subjects, and so on. You import different databases into separate namespaces to avoid duplicate names.

passport

Session-based information regarding authenticated users. A passport is created the first time a user accesses Cognos 8. It is retained until a session ends, either when the user logs off, or after a specified period of inactivity.

Passport information is stored in Content Manager memory. Credentials are stored encrypted.

A passport is stored in a memory-only browser cookie for the duration of the session.

portlet

A mechanism for displaying Web content as part of a portal page.

product locale

The code or setting that specifies what language, regional settings, or both to use for parts of the product interface, such as menu commands.

prompt

A report element that asks for parameter values before the report is run.

report specification

The definition of queries, prompts, layouts, and styles that make up a report. A report specification is combined with data by a run operation to create report outputs. You create report specifications by using Report Studio, Query Studio, Analysis Studio, or through the Software Development Kit.

response file

An ASCII file that contains the setup data that is needed to automate an installation. For Cognos installations, the response file automates only the process of copying files with the default configuration.

security provider

See authentication provider.

user

A person accessing a Cognos 8 application. Authenticated user definitions and information, such as passwords and IDs, are maintained in third-party authentication sources.

Other user information, such as the location of personal folders or preferred formats for viewing reports, is stored in Cognos 8.

Index

A

accented characters
  not displayed properly, 385
acceptCount
  increasing for Apache Tomcat, 352
access permissions
  definition, 399
Active Directory Server
  advanced properties, 261
  authenticating in multiple domains, 261
  enabling single signon, 262
  enabling SSL, 260
  missing group membership, 393
  using for authentication, 257
  with an LDAP namespace, 271
active scripting
  enabling in Web browsers, 135
agent service, 350
aggregation
  samples and time dimensions, 325
AIX
  environment variables to install Cognos 8, 99
  error connecting to DB2 database, 376
aliases
  configuring on Apache Web Server, 231
  configuring on Web servers, 132
  definition, 399
Analysis Studio
  changes after upgrading, 17
  component description, 22
anonymous access
  definition, 399
  disabling, 244
  enabling for PowerPlay report data in Cognos 8 Go! Office, 240
anonymous logon
  disabling, 256
  disabling for Portal Services, 244
apache_mod file
  configuring for gateways, 177
Apache Derby
  migrate to content manager database, 64
Apache gateways
  configuring, 231
Apache Tomcat
  tuning, 352
Apache Web servers
  configuring aliases, 132
  configuring as gateways, 231
application servers
  changing from the default, 293
  configuring, 303
  servlet class fails to load in WebLogic, 396
  servlet gateways, 233
  single signon for WebSphere Portal, 252
  startup script fails, 382
  startup scripts, 301
  startup scripts for Oracle application server, 307, 308
  upgrading Cognos 8, 311
application tier components
  configuration requirements, 30, 40
  configuring, 167
  definition, 399
  installing on separate computer, 30
  installing on separate computer for Cognos 8 scorecarding, 39
Application Tier Components
  log server, 215
  workflow for installing and configuring, 89
Architect models
  migration to Cognos 8, 45
archiving
  report output, 210
audience of document, 11
audit
  logs, 215
audit logs
  log destinations, 215

See Also log messages
See Also troubleshooting
authentication
Active Directory Server, 257
configuring Cognos Series 7 namespace, 263
custom authentication providers, 268
custom properties for Active Directory Server, 259
custom user properties for LDAP, 280
definition, 399
deleting namespaces, 291
disabling anonymous logon, 256
domain trees for Active Directory Server, 261
eTrust Siteminder, 283, 285, 286
LDAP, 268, 269
LDAP using Active Directory Server, 271
LDAP using IBM Directory Server, 273
LDAP using Novell Directory Server, 275
LDAP using Sun Java System Directory Server, 278
NTLM, 286
requirements for single signon with Microsoft Analysis Server or Microsoft SQL Server, 258
SaferAPIGetTrustedSignon function, 266
SAP, 288
single signon for NTLM, 287
single signon for Plumtree Portal using HTTP Basic authentication, 253
single signon using Active Directory Server, 262
single signon using Cognos Series 7 namespace, 265
single signon using eTrust SiteMinder, 286
single signon using LDAP, 282
single signon using SAP, 290
SSL for eTrust Siteminder, 286
SSL using LDAP, 281
testing namespaces, 291
trusted signon plug-ins for Cognos Series 7, 265
using namespaces, 255
authentication providers
definition, 399

B

backing up
Cognos 8 information, 295, 314
backslashes appear instead of currency, 223
batch report service, 350
Batch report service
list of embedded fonts for PDF reports, 208
BEA WebLogic, 293
BI bus
upgrade considerations, 57
Bind user DN and password property
special characters for LDAP namespace, 268
BMTScriptPlayer
availability on Linux, 98
builds
running in Cognos Connection by using Data Movement service, 47

C

CA, *See* certification authority
calendars
upgrading Metrics Manager custom calendars, 77
CAM-CRP-1157 error, 370
certificates
definition, 399
certificate signing requests
generating, 317
certification authority
configuring the service, 317
definition, 399
CGI gateway
limitations with multiple Content Manager computers, 158
CGI timeout error, 395
changing
Cognos 8 gateway, 231
configuration template, 204
default configuration settings, 193
email encoding, 228
Java versions, 314
type of JVM, 313
URIs, 196
characters
encoding not supported, 371
characters improperly displayed, 385
chase_referral files, 261
Chinese
characters display incorrectly after upgrade, 384
chunking patches
application servers, 295
cipher suites
definition, 400
setting a priority for SSL connections, 214

client computers
workflow for configuring, 90
Client software
installing, 82, 240
code pages for data sources, 138
Cognos
samples, 328
Cognos 8
changing application servers, 293
components, 21
configuring, 137
default settings, 93
deploying, 303
dispatchers, 351
installation options, 27
installing, 98
running on same computer as ReportNet, 77
service does not start, 370
services, 351
sharing components on same computer, 31
system requirements, 94
troubleshooting installations, 365
uninstalling, 113
workflows, 88
Cognos 8 Controller
considerations when upgrading Cognos 8 BI, 58
Cognos 8 G0! Office
uninstalling, 81
Cognos 8 Go! Office
changed features, 16
component description, 22
configuring, 237
content type settings for your Web server, 238
deploying the client components, 240
error using Run Reports, 394
macro seciurity level for Microsoft Office XP, 242
MIME type settings for your Web server, 238
SSL, 239
template files, 237
testing the installation of client components, 242
upgrading, 81
using PowerPlay reports, 240
virtual directories, 237
Cognos 8 Go! Search
using to search Cognos 8 BI content, 47
Cognos 8 samples, 23
Cognos 8 scorecarding
distributing components, 37
installing Application Tier Components on separate computer, 39
installing components on one computer, 38
installing gateway on separate computer, 38
Cognos 8 server
fails to start, 371
Cognos 8 service
configuring, 204
requirements for the user account that is used for the service, 145
server not available, 371
starting, 391
starting from Cognos Configuration, 151, 191
starting from the command line, 360
stopping from the command line, 360
Cognos 8 Transformer
setting up data sources, 138
setting up the database client, 127
Cognos Administration
component description, 21
Cognos Application Firewall
configuring, 201
Cognos Configuration
component description, 22
font not found error on UNIX, 392
invalid settings, 371
problems opening, 366
problems saving a configuration, 385
problems with keyboard navigation, 389
trouble generating cryptographic keys after install, 388
unable to start, 389
unattended mode, 346
Cognos Connection
component description, 21
unable to open, 378
Cognos Content Database
changing users and passwords, 194
component description, 23
content store, 123
improving performance, 353
uninstalling, 115
Cognos Controller
data access in Cognos 8, 46

Cognos DecisionStream
requirements to upgrade catalogs to Cognos 8, 44
Cognos Finance
data access in Cognos 8, 46
Cognos Go! Mobile
mobile reports, 47
Cognos Metrics Manager
requirements to upgrade to Cognos 8, 44
upgrading saved reports from version 2.x to Cognos 8, 56
upgrading to Cognos 8, 44, 55
Cognos namespace
recreating, 389
Cognos NoticeCast
duplication of functionality in Cognos 8, 48
Cognos Office Connection, *See* Cognos 8 Go! Office
Cognos Planning - Analyst
data access in Cognos 8, 46
Cognos Planning - Contributor
data access in Cognos 8, 46
enabling scheduled reports and agents, 234
migration to Cognos 8, 45
Cognos Portal Services
migration overview, 48
Cognos PowerPlay Web
requirements to upgrade reports to Cognos 8, 44
Cognos Query
duplication of functionality in Cognos 8, 48
Cognos samples, 328
CognosScript
migration overview, 48
Cognos Series 7
enabling single signon, 265
enabling SSL, 264
migration to Cognos 8, 45
trusted signon plug-ins, 265
using for authentication, 263
Cognos Series 7 PowerCubes
publishing after upgrade, 80
requirements for successful language conversion, 46
Cognos Series 7 Transformer models
preparing for upgrade to Cognos 8, 83
Cognos Viewer
component description, 21
Cognos Visualizer
duplication of functionality in Cognos 8, 48
Cognos Web Services
migration overview, 48
cogstartup.lock file, 366
cogstartup.xml file, 356, 360
changing properties manually, 358
invalid file, 390
collation sequences
case-sensitive, 371
COM add-ins for Cognos 8 Go! Office
updating, 240
common gateway interface
replacing, 231
common gateway interface (CGI)
definition, 400
common symmetric key, 199
components, 21
Analysis Studio, 22
application tier components, 30
Cognos 8 Go! Office, 22
Cognos 8 samples, 23
Cognos Administration, 21
Cognos Configuration, 22
Cognos Connection, 21
Cognos Content Database, 23
Cognos Viewer, 21
Composite Information Server, 23
Content Manager, 22, 31, 40, 98
content store, 24
data sources, 25
distributing Metric Designer, 41
Event Studio, 22
Framework Manager, 23
gateways, 22, 29, 98
installing, 98
installing on one computer, 28
Map Manager, 24
Metric Designer, 23
metric store, 24
Metric Studio, 22
Query Studio, 22
report server, 98
Report Studio, 21
third-party, 21
Transformer, 24

components for Cognos 8 scorecarding
installing Application Tier Components on separate computer, 39
installing gateway on separate computer, 38
installing on one computer, 38
Composite Information Server
component description, 23
Confidentiality algorithm, 201
configuration
adding resources, 356
advanced options, 313
automating, 343
backing up, 295, 314
changing defaults settings, 193
changing the template, 204
Content Manager, 31, 40
cryptographic information cannot be encrypted, 387
data locked, 389
default settings, 193
error when encrypting information, 387
global settings, 221
in silent mode for upgrade, 72
lock file, 366
manual, 355
requirements for Metric Designer, 43
requirements for single signon with Microsoft Analysis Server or Microsoft SQL Server, 258
running from command line, 360
running multiple versions of Cognos 8, 77
settings for Cognos 8, 104, 193
settings not applied, 391
testing, 152, 192
Tomcat settings, 104
unable to open Cognos Configuration, 366
unable to save, 389
unattended, 343, 346
upgrade considerations, 58, 66
workflows, 87
configuration files
applications.xml for Portal Services, 243
coglocale.xml, 359
cogstartup.xml, 356
exporting, 346
configuration issues, 385
configuring
Active Directory namespace, 258
apache_mod for the gateway, 177
application server properties, 303
application tier components, 167
certificate authority service, 317
Cognos 8, 137
Cognos 8 for application servers, 298
Cognos 8 Go! Office, 237
Cognos 8 service, 204
Cognos 8 to work with other Cognos products, 234
Content Manager computers, 158
custom authentication providers, 268
default time zone, 228
destination for log messages, 215
distributed installations, 156
environment properties for application tier components, 169
eTrust SiteMinder namespace, 285
fonts, 205
Framework Manager, 32, 176
Framework Manager on different computer, 177
gateways, 171
ISAPI for the gateway, 177
JDBC drivers, 127
LDAP namespace, 269
LDAP namespace for Active Directory Server, 271
LDAP namespace for IBM Directory Server, 273
mail server, 149, 162, 167
map charts for Report Studio, 210
Metric Designer, 188
NTLM namespace, 287
Portal Services, 243
properties in an unattended configuration, 358
required tasks, 146, 156
routers, 138
SAP namespace, 289
servlets for the gateway, 177
shared trust with other servers, 213
single computer installations, 146
SSL protocol, 211
standby Content Manager, 163
temporary file location, 202
transfer specification files (.ats), 343
Transformer, 34, 181
unattended, 346
Web browsers, 135
Web server, 132

connections
data source connections, 330
definition, 400
OLAP data sources, 333
content expiry
images directory, 132
content locale
definition, 400
content locales
customizing, 224
mapping to user locale, 225
content manager
migrate from Apache Derby, 64
Content Manager
an attempt to register the dispatcher, 376
changing time zones, 228
component, 31, 40
component description, 22
configuration, 31, 40
configuring, 158
configuring on multiple computers, 163
default active, 158
definition, 400
failover protection, 31, 40
installation options, 31, 40
installing, 98
log server, 215
requirements for changing application server, 295
requirements if using Cognos 8 Transformer with Series 7 namespace, 98, 108, 263
setting up a content store, 118
standby, 31, 40
upgrade considerations, 56
workflow for installing and configuring, 89
Content Manager service, 350
Content Manager URIs, 163, 169
content store
and other locations to store report output, 209
backing up, 295, 314
Cognos Content Database, 123
compatible versions of DB2 and Java, 370
component description, 24
connection management, 147, 159
creating, 93, 118
DB2, 120
definition, 400
deleting tables from the database, 385
error initializing in Oracle, 395
importing data, 311, 317
invalid settings, 371
JDBC drivers, 127
Microsoft SQL Server, 118
Oracle, 120
requirements for changing application server, 295
setting up database clients, 127
Sybase Adaptive Server Enterprise, 122
upgrading, 56, 376
context attribute cannot be deserialized, 383
context error, 383
Controller, *See* Cognos 8 Controller
cookies
customizing, 230
enabling in Web browsers, 135
settings, 230
copyright material
printing, 13
creating
content store, 93
data source connections to metric store, 154, 174
metric package, 154, 174
metric store, 124
credentials
definition, 400
cross-script checking
configuring in Cognos Application Firewall, 201
cryptographic error, 390
cogstartup.xml file invalid, 390
JRE error, 390
problems after upgrading, 388
cryptographic information cannot be encrypted, 387
cryptographic keys
backing up and deleting, 295, 314
generating for third-party certificate authorities, 317
regenerating, 388
cubes
cannot open, 377
upgrading a secured cube, 85
upgrading PowerCubes, 83
currency
customizing support, 222
won, 223
yen, 223

custom authentication providers, 268
custom user properties
  Active Directory Server, 259
  LDAP, 280

D

data
  Cognos samples, 328
  locked by Cognos Configuration, 389
database client
  requirements for Transformer, 36
  requirements for Transformer modelers, 185
  setting up, 127
  setting up for a logging database, 217
database connections, *See* data source connections
database connection strings
  IBM DB2, 147, 159
  Microsoft SQL Server, 147, 159
  Oracle, 147, 159
database connectivity
  content store, 97
  metric store, 97
  query database, 96
  reporting database, 96
databases
  bulk load utility missing, 394
  Cognos samples, 328
  content store, 118
  deleting tables, 385
  logging, 217
  logging, creating, 118
  logging, testing, 152, 192
  logging database client, 217
  metric store, 124
  notification, 149, 162
  returning to original state in Event Studio, 340
Data files location
  configuring for Windows Vista, 150, 165, 169, 173
data integration service, 350
Data Manager
  using in Cognos 8 BI, 47
Data Movement service
  using in Cognos Connection, 47
data source connections
  metric stores, 154, 174
  setting, 147, 159
data sources
  component description, 25
  definition, 401
  for Cognos 8 Transformer, 138
  for Framework Manager, 138
  for Metric Designer, 138
  ODBC connections, 142
  samples connections, 330
data store, *See* metric store
DB2, 378
  code pages, 138
  content store, 120
  database connectivity, 96, 97
  environment variables, 120
  JDBC drivers, 129
  metric store, 126
  setting up JDBC drivers, 218
  supported Java versions, 370
DB2 content store, 352
DB2-ERR-0028, 392
DB2 OLAP
  unable to load library, 392
DecisionStream
  requirements to upgrade catalogs to Cognos 8, 44
DecisionStream to Cognos 8
  upgrade consideration, 44
deleting
  Cognos samples, 341
delivery
  decreasing the time to open reports, 354
delivery service, 350
demonstration environments, 146, 176
deploying
  Cognos 8, 394
  failure on Oracle or WebSphere Application Server, 382
  Transformer for modelers, 187
deploying Cognos 8, 303
deployment archives
  definition, 401
Deployment files location
  configuring for Windows Vista, 150, 165, 169, 173
Derby
  page cache size, 353
diagnostics, *See* troubleshooting
directory not found error, 378

disabling
anonymous access, 244
content maintenance job, 338
dispatcher
changing properties file, 303
does not start on Application Tier Components computer, 396
unregistering, 310
dispatchers
system metrics, 349
distributed installations
configuring, 156
configuring Framework Manager, 177
configuring Transformer, 181
installation and configuration workflows, 91
Metric Designer, 41
scenarios, 27, 37
domains
Active Directory Server domain trees, 261
setting for cookies, 230
double-byte characters
improperly displayed, 385
download of resource fails, 376
DPR-DPR-1035 error, 370

E

EAR files, *See* Enterprise archive files
EBA-090034 Error
on WebLogic 8, 380
email messages
changing the encoding, 228
embedded fonts, 208
enabling
Cognos Application Firewall, 201
services, 203
SSL for an application server, 310
encryption
changing settings in unattended configuration, 358
configuration errors, 387
Enterprise archive files
deploying Cognos 8, 361
environments
supported, 98
environment variables
configuring for application tier components, 169
configuring for Metric Designer, 189
content store, 118
DB2, 120
for Oracle data source, 106
for Transformer on Linux and UNIX, 109
Oracle, 120
requirements on Windows Vista, 150, 165, 169, 173
setting for application servers, 297
setting up on UNIX for metric store, 130
to install Cognos 8 on UNIX or Linux, 99
error messages
CAM-CRP-1064, 375
CAM-CRP-1315 Current configuration points to a different trust domain, 388
CFG-ERR-0106 Cognos Configuration received no response, 368
CGI timeout, 395
CM-CFG-029 Content Manager is unable to determine, 391
CMM-APP-3254 The initialization of the metrics store failed, 394
corrupt cryptographic information, 390
could not deserialize context attribute, 383
cryptographic information cannot be encrypted, 387
DIS-ERR-3115 Task execution failed, 394
download of specified resource fails, 376
DPR-ERR-2022 No response generated, 381
DPR-ERR-2058, 376, 378
HTTP Error 404, 378
Java Runtime Environment, 390
malformed request, 384
MDS-RUN-3213 Unable to locate database bulk load utility, 394
page not found, 378
PRS-CSE-1255, 375
servlet class fails to load on WebLogic, 396
SoapSocketException, 376
SQL1224N, 376
you have chosen to download a file, 381
errors
DB2-ERR-0028, 392
Essbase, 378
eTrust SiteMinder
configuring namespaces, 285
cross-script checking in Cognos Application Firewall, 201
enabling single signon, 286

protecting the Cognos 8 Web alias, 286
SSL, 286
using for authentication, 283
event logs, 217
event management service, 350
Event Studio
component description, 22
returning databases to original state, 340
samples, 339
Excel
multipage report type does not work, 383
exporting
configuration files, 346
external identity mapping property
editing for an LDAP namespace, 283
External identity mapping property
special characters for LDAP namespace, 268

F

failover protection, 31, 40
ISAPI gateway required for multiple Content Manager installation, 158
file locations
requirements on Windows Vista, 150, 165, 169, 173
files
not found, 378
file system
to save copies of report output, 209
finding information, 12
Firefox
browser settings, 135
firewalls
access between Framework Manager and Cognos 8, 177
access between Transformer and Cognos 8, 181
installation considerations, 32, 35, 42
flicker, 397
font embedding lists, 208
fonts
changing for PDF reports, 207
changing the default, 207
configuring, 205
list of embedded fonts for PDF reports, 208
not found when starting Cognos Configuration on UNIX, 392
Framework Manager
accessing Cognos 8 outside a firewall, 177
component description, 23
configuring, 32, 176
configuring on different computer, 177
configuring source control systems, 178
installation options, 32
installing, 105
sample models, 338
setting up data sources, 138
setting up the database client, 127
system requirements, 105
testing installation and configuration, 153, 193
unable to load DB2 OLAP library, 392
uninstalling, 114
upgrade considerations, 57

G

gateway
configuring for Transformer, 181
log file, 367
recommended settings for Microsoft IIS, 395
when to use ISAPI, 395
workflow for installing and configuring, 89
gateways
adding in a network to decrease delivery times, 354
component description, 22
configuration requirements, 29, 39
configuring, 171
configuring apache_mod, 177
configuring a servlet, 177
configuring for Cognos 8, 231
configuring ISAPI, 177
configuring to use a namespace, 203
definition, 401
installing, 98
installing on separate computer, 29
installing on separate computer for Cognos 8 scorecarding, 38
Global Customer Services Web site, 13
glyphs
definition, 401
Great Outdoors, *See* Cognos samples
Great Outdoors samples, 23, 323
installing, 102

groups
definition, 401
missing membership in Active Directory Server, 393

H

help
getting, 13
HP-UX
environment variables to install Cognos 8, 99
HTML cookies, *See* cookies
HTTP Basic authentication
for single signon with Plumtree Portal, 253
HTTP Error 404, 378
HTTPS
definition, 401

I

IBM DB2
creating connection strings, 147, 159
IBM Directory Server
with an LDAP namespace, 273
IBM WebSphere, 293
IIS Web servers
single signon for PowerPlay report based Cognos 8 Go! Office documents, 240
single signon using Active Directory, 262
images
content expiry, 132
loading in Report Studio, 132
importing
MDL files from Cognos Series 7, 84
samples, 336
Impromptu catalogs and reports
migration to Cognos 8, 45
Impromptu Web Reports
migration to Cognos 8, 45
information
finding, 12
installation
checklist, 93
options for Content Manager, 31, 40
options for Framework Manager, 32
options for Transformer, 34
testing, 152, 192
unattended, 343
workflows, 87
installation and configuration issues
cannot load DB2 OLAP library, 392
installation file
downloading for Transformer modelers, 185
installing
Cognos 8, 93, 98, 343
Cognos 8 on Linux, 385
Framework Manager, 105
Great Outdoors samples, 102
in an environment that includes Cognos 8 Controller, 58
Metric Designer, 111
on a single computer, 88
on multiple computers, 89
Transformer, 17, 108
unattended install, 343
using transfer specification file (.ats), 343
using transfer specification files (.ats), 343
Integrated Windows Authentication
issues, 391
interface
customizing language support, 221
Internet Explorer
browser settings, 135
invalid cogstartup.xml file, 390
invalid settings
Cognos Configuration, 371
content store, 371
ISAPI
accessing Cognos 8, 231
configuring for gateway, 177
when to use for a gateway, 395
ISAPI gateway
required with multiple Content Manager computers, 158

J

Japanese
characters display incorrectly after upgrade, 384
Japanese currency, 223
jar file, 131
error when starting configuration, 390
Java
changing versions, 314

configuring servlet gateway for Java-compatible Web servers, 233
supported versions for DB2 content store, 370
types of virtual machine, 313
updating runtime environments, 131, 298, 316
uses all of CPU, 370
JAVA_HOME
setting, 390
Java Archive files, *See* jar file
Java error when starting configuration, 390
Java scripts
enabling in Web browsers, 135
Java System Web Server
configuring aliases, 132
JDBC, 127
content store, 96
database connectivity for content store, 97
DB2, 129
metric store, 97
Oracle databases, 128
JDBC drivers
setting up DB2 databases, 218
setting up Oracle databases, 218
jobs
definition, 401
job service, 350
job steps
definition, 401
JobStreams
running in Cognos Connection by using Data Movement service, 47
JREs
updating, 131, 298, 316
JVM
changing, 295, 314
copying security provider files, 131, 298, 316
memory settings for Cognos Content Database, 353

K

keyboard
navigation problems, 389
Korean
characters display incorrectly after upgrade, 384
Korean currency, 223

L

language
conversion tables, 384
customizing for user interface, 221
customizing locale content support, 224
incompatibility after upgrade, 384
latency
improving, 354
LDAP
Active Directory Server, 271
configuring a namespace, 269
custom properties, 280
editing the External identity mapping property, 283
enabling single signon, 282
enabling SSL, 281
IBM Directory Server, 273
Novell Directory Server, 275
Sun Java System Directory Server, 278
using for authentication, 268
Linux
characters not displayed properly, 385
environment variables for Cognos 8, 99
environment variables for Tranformer, 109
log messages, 217
ODBC connections to data sources, 142
starting and stopping the Cognos 8 service, 360
system requirements, 93
unsupported features and components, 98
load balancing, 137
configuring mail server settings, 149, 162, 167
enabling and disabling services, 203
setting, 30, 39
locales
definition, 402
locations
map charts, 210
log database
deleting tables, 385
log destinations
types of, 215
log files, 365
for gateway errors, 367
locale configuration, 366
run-time, 366
silent mode, 367

startup configuration, 366
transfer, 365
transfer summary, 366
uninstallation, 367
logging
configuring, 219
database, 217
database client, 217
remote log servers, 217
using files, 217
logging databases
creaating, 118
creating, 118
testing, 152, 192
log messages
enabling for Cognos Application Firewall, 201
log destinations, 215
remote log server, 215
See Also audit logs
See Also troubleshooting
logs
message processing, 215
service, 351

M

mail server
configuring, 149, 162, 167
maintenance
improving system performance, 349
map charts, 210
Map files location
configuring for Windows Vista, 150, 165, 169, 173
Map Manager
component description, 24
maxProcessor
increasing for Apache Tomcat, 352
MDL files
importing from Cognos Series 7, 84
Metric Designer
component description, 23
configuration requirements, 43
configuring, 188
distributing components, 41
installing, 111
setting up data sources, 138
system requirements, 112
testing installation and configuration, 154, 193
uninstalling, 114
upgrading project, 57
metric packages
creating, 154, 174
definition, 402
metrics
for servers, dispatchers, and services, 349
Metrics Manager
uninstalling, 72
upgrading, 72
upgrading custom calendars, 77
upgrading security information, 73
Metrics Manager service, 351
metric store
component description, 24
creating, 124
creating data source connections, 154, 174
database connectivity, 97
DB2, 126
failure, 394
improving performance, 353
JDBC drivers, 127
Microsoft SQL Server, 124
Oracle, 124, 126
setting up database clients, 127
setting up environment variables on UNIX, 130
upgrading, 57, 155, 175
metric stores
definition, 402
Metric Studio
component description, 22
creating metric package, 154
installation and configuration workflows, 90
Microsoft
security update affects memory, 371
Microsoft .NET Framework, 240
Microsoft Analysis Server
namespace requirement, 258
Microsoft Analysis Services
setting up MSAS cube samples, 332
setting up the data source environment, 138
single signon to MSAS data sources, 262
Microsoft IIS Web servers
recommended gateway settings, 395

Microsoft Office
report data service, 351
Microsoft Office Excel
multipage report type does not work, 383
Microsoft SQL Server
content store, 118
creating connection strings, 147, 159
database connectivity, 96, 97
metric store, 124
namespace requirement, 258
migration
from other Cognos products to Cognos 8, 45, 54
Migration service, 351
MIME types
for Cognos 8 Go! Office, 238
Mircrosoft .NET Framework
updating, 82, 240
mobile devices
using to access reports, 47
modelers
deploying Transformer, 187
modeling
sample models and packages, 326
modeling components, 23
installation file for Transformer modelers, 185
models
database samples, 338
importing from Cognos Series 7 Transformer, 84
modifying for samples, 336
monitor service, 351
Moving from trial upgrade to production environment, 53
MSAS, 378
MSAS, *See* Microsoft Analysis Services
MS Cube, 377
multi_domain_tree, 261

N

namespace
Active Directory Server missing group membership, 393
cannot log on, 375
recreating, 389
namespaces
authentication, 255
configuring custom authentication providers, 268
configuring for a gateway, 203
definition, 402
deleting, 291
requirements for Content Manager if using Transformer with Series 7 namespace, 98, 108, 263
testing, 291
Netegrity SiteMinder, *See* eTrust SiteMinder
Netezza
setting up ODBC connections, 142
Netscape
browser settings, 135
network outage
services fail to start, 375
New Metric Package wizard
upgrading metric store, 155, 175
no response generated, 381
notification database, 162, 167
deleting tables, 385
Novell Directory Server
with an LDAP namespace, 275
NTLM, 286
configuring, 287
enabling single signon, 287
NTLM, *See Also* Windows native security (NTLM)

O

ODBC connections for data sources, 142
OLAP data sources, 377, 378
connections, 333
members missing or inaccessible, 393
operating systems
affect on upgrade, 58
Oracle
application server, 307, 308
content store, 120
creating connections strings, 147, 159
database connectivity, 96, 97
database JDBC drivers, 218
deployment errors, 394
environment variables, 120
environment variables for data source, 106
environment variables for metric store on UNIX, 130
JDBC drivers, 128
metric store, 124, 126
multilingual support, 138

Oracle application server, 293
Oracle Application Server
  Cognos 8 deployment failure, 382
  deploying Cognos 8, 394
Oracle content store
  compatibility levels, 395
  error initializing, 395

P

p2pd.war file for WebLogic, 383
page cache size
  Derby, 353
page not found error
  starting Cognos 8 in Windows 2003, 378
passports
  definition, 402
passwords
  changing for Cognos Content Database, 194
  changing in unattended configuration, 358
paths
  setting for cookies, 230
PDF fonts
  mapping to built-in PDF fonts for faster report printing, 206
performance
  improving for Apache Tomcat, 352
permissions
  for the user account that is used for the Cognos 8 service, 145
  for Transformer modelers, 185
planning an upgrade, 50
Plumtree Portal
  single signon using HTTP Basic authentication, 253
  single signon using SiteMinder, 253
pop-up blocking, 381
portal
  errors in starting, 378, 381
portal problems
  unable to open, 378
Portal Services, 243
  availability on Linux, 98
  disabling anonymous logon in Cognos 8, 244
  specifying the applications.xml file, 243
portlets
  definition, 402
ports
  changing, 196
  default configuration settings, 104
  running multiple versions of Cognos 8, 77
ports already in use, 369
PowerCubes
  access in Cognos 8, 46
  cannot open, 377
  published from Cognos Series 7 after upgrade, 80
  requirements for successful language conversion, 46
  Series 7, 85
  upgrading, 83
PowerPlay
  considerations for upgrading to Cognos 8, 44, 54
  enabling anonymous access for Cognos 8 Go! Office, 240
  migrating PowerPlay Web reports to Cognos 8, 45
PowerPlay Web
  requirements to upgrade reports to Cognos 8, 44
presentation service, 351
Presentation service
  requirements, 349
printing copyright material, 13
problems opening Cognos Configuration, 366
processing log messages, 215
product locale
  definition, 402
product locales
  mapping for user interface, 227
projects
  upgrading Metric Designer projects, 57, 190
prompts
  definition, 402
proof of concept, 146, 176
properties
  changing in unattended configuration, 358
  configuring for application server, 303
  temporary file location, 202
properties file
  for dispatcher, 303

Q

quality of protection in SSL connections, 214
query databases, 25
Query Studio
  changes after upgrading, 17

component description, 22
quick tours
using, 13

R

readme
reviewing before you install, 93
recreating the Cognos namespace, 389
related documentation, 11
relational data sources
members missing or inaccessible, 393
remote log servers, 217
configuring, 219
report data service, 351
report distribution
on a network, 354
reporting needs
for Transformer users, 36
ReportNet
requirements to upgrade to Cognos 8, 44
running on same computer as Cognos 8, 77
to Cognos 8 upgrade file, 367
unable to uninstall service, 79
upgrading, 44, 55
upgrading to Cognos 8, 55
report output
reusing, 210
saving to a file system, 209
sharing with users outside Cognos 8, 209
reports
changing default font, 207
customizing language support, 224
decreasing delivery time, 354
testing before an upgrade, 53
report servers
installing, 98
Report service
list of embedded fonts for PDF reports, 208
requirements, 349
report services, 351
report specifications
definition, 403
Report Studio
changes after upgrading, 17
change the location of map charts, 210
component description, 21
does not start, 381
loading images, 132
required tasks
configuring, 146, 156
requirements
for installing Cognos 8 Go! Office, 81
resources
adding, 356
response.ats file, 343
response files
definition, 403
restoring
samples databases, 329
reviewing the readme before you install, 93
role-based servers
considerations for Transformer, 36
root directory
for saving report output outside Cognos 8, 209
routers
configuring, 138

S

SaferAPIGetTrustedSignon function
using for authentication, 266
samples, 23
data source connections, 330
DB2 Cube, 332
deleting, 341
Event Studio, 339
general employee information, 325
general financial information, 324
general sales and marketing information, 325
GO data warehouse, 326
GO Sales transactional database, 327
Great Outdoors, 323
Great Outdoors company structure, 324
importing, 336
installing, 102
Metric Designer, 328
Metric Studio, 335
model design, 326
models, 338
MSAS cube, 332
OLAP data sources, 333
restoring samples databases, 329
setting up, 328

SAP
application server, 293
enabling single signon, 290
using for authentication, 288
SAP BW
authorization settings for Cognos 8 administrators, 289
authorization settings for Cognos 8 users, 288
connectivity, 289
screen flicker, 397
scripts
to delete tables from databases, 385
to improve metric store performance, 353
SDK applications
upgrade considerations, 56
searching Cognos 8 BI content, 47
secure flag
setting for cookies, 230
secure LDAP communication, 281
Secure Sockets Layer, *See* SSL protocol
security
issues with Integrated Windows Authentication, 391
settings for Web browsers, 94
upgrading Metrics Manager, 73
security provider files
copying to application server JVM, 131, 298, 316
security providers
definition, 403
Series 7
upgrading to Cognos 8, 54
Series 7 IQD Bridge
installing, 108
Transformer component, 24
Series 7 PowerCubes
requirements for successful language conversion, 46
Series 7 PowerPlay
upgrading saved reports from ReportNet to Cognos 8, 56
Series 7 secured cubes
opening, 85
upgrading, 85
Series 7 Transformer models
preparing for upgrade to Cognos 8, 83
server components, 21
servers
system metrics, 349
server time zones
changing, 228
services
adjusting to improve performance, 349
agent, 350
batch report, 350
Cognos 8, 351
Content Manager, 350
data integration, 350
delivery, 350
enabling and disabling, 203
event management, 350
fail to start after network outage, 375
job, 350
log, 351
Metrics Manager, 351
Migration, 351
monitor, 351
presentation, 349, 351
report, 351
Report, 349
report data, 351
starting from the command line, 360
stopping from the command line, 360
system, 352
system metrics, 349
unable to start, 369
uninstalling, 113
servlet gateway
configuring, 233
setting
data source connections, 147
setting up
samples, 328
shared secret
single signon for Portal Services, 245
shared trust
setting up between Cognos 8 and other servers, 213
silent configurations, *See* unattended configurations
silent installations, *See* unattended installation
silent mode, *See* unattended mode
single computer installation
configuring, 146
installation and configuration workflows, 88, 90
single signon
Active Directory namespace, 262

enabling access to Cognos 8 Go! Office documents based on PowerPlay reports, 240
eTrust SiteMinder user directory, 286
for Plumtree Portal using HTTP Basic authentication, 253
for Plumtree Portal using SiteMinder, 253
for WebSphere Portal using application server, 252
issues with Integrated Windows Authentication, 391
LDAP namespace, 282
NTLM namespace, 287
SAP namespace, 290
using Cognos Series 7 namespace, 265
using shared secret for Portal Services, 245
SiteMinder
single signon for Plumtree Portal, 253
site surveys, 51
smart client
removed from Cognos 8 Go! Office, 16
Solaris
environment variables to install Cognos 8, 99
source control systems
configuring for Framework Manager, 178
special characters
in LDAP namespace properties, 268
SQL Server databases
creating content store, 118
SSL
Active Directory Server, 260
additional steps to configure on WebLogic 8, 380
configuring for Cognos 8 Go! Office, 239
enabling for an application server, 310
enabling on Web servers, 133
eTrust SiteMinder user directory, 286
LDAP namespace, 281
quality of protection, 214
setting up shared trust with other servers, 213
using Cognos Series 7 namespace, 264
SSL protocol
configuring, 211
standby Content Manager, 31, 40
configuring, 163
starting
the Cognos 8 service from Cognos Configuration, 151, 191
starting the Cognos 8 service
from the command line, 360
startup
Cognos 8 service, 391
configuration lock file, 366
DB2 returns SQL1224N error when connecting from AIX, 376
download of resource fails, 376
page not found, 378
problems, 367
Report Studio does not start, 381
script fails, 382
unable to download cognos.xts, 381
unable to open Cognos Connection, 378
unable to start service, 369
Startup
failure without error, 371
startup scripts, *See Also* application servers
stopping the Cognos 8 service
from the command line, 360
Sun Java System Directory Server
with an LDAP namespace, 278
supported environments, 98
Sybase
database drivers, 129
Sybase Adaptive Server Enterprise
content store, 122
Sybase IQ
setting up ODBC connections, 142
syslog
destination for log messages, 217
system requirements, 94
Framework Manager, 105
Metric Designer, 112
Transformer, 108
system service, 352

T

Tab key
problems in Cognos Configuration, 389
tables
deleting from a database, 385
tablespaces, 352
template
changing the size of template, 204
temporary directories
deleting before reinstall, 388

temporary file location
configuring, 202
properties, 202
Temporary files location
configuring for Windows Vista, 150, 165, 169, 173
testing
Cognos 8 Go! Office installation, 242
configuration, 152, 192
installation, 152, 192
Thai email encoding
JRE requirements, 228
third-party certificate authority
configuring, 317
third-party components, 24
third-party products
upgrading, 77
third-party software
upgrade concerns, 51
time zones
changing, 228
Tomcat
default configuration settings, 104
tuning, 352
transfer specification files (.ats)
configuration, 343
Transformer
accessing Cognos 8 outside a firewall, 181
component description, 24
component for linking to IQD files from Series 7, 24
configuring, 34, 181
data access in Cognos 8, 46
deploying for modelers, 187
environment variables on Linux and UNIX, 109
installation options, 34
installing, 108
new features in Cognos 8, 17
preparing Series 7 models for upgrade to Cognos 8, 83
requirements for Content Manager if using Series 7 namespace, 98, 108, 263
steps to test installation, 154, 193
system requirements, 108
uninstalling, 114
upgrading cubes, 83
Transformer installation file, 185
Transformer models
importing from Cognos Series 7, 84
trial upgrade, 53
planning the move to the production environment, 53
troubleshooting, 365
logging, 215
trust domain error
when saving the configuration, 388
tuning
Apache Tomcat settings, 352
DB2 content store, 352

U

UDB, *See* DB2
unable to open Cognos Configuration, 366
unattended configuration
changing properties, 358
setting up, 343
unattended configurations
upgrading, 72
unattended installation
setting up, 343
unattended mode, 343
uninstalling
Cognos 8, 113, 114
Cognos 8 Go! Office, 81
Cognos Content Database, 115
Framework Manager, 114
Metric Designer, 114
Metrics Manager, 72
ReportNet service, 79
Transformer, 114
UNIX
environment variables for Cognos 8, 99
environment variables for Oracle data source, 106
environment variables for Tranformer, 109
font not found error, 392
log messages, 217
ODBC connections to data sources, 142
setting up environment variables for metric store, 130
starting and stopping the Cognos 8 service, 360
system requirements, 93
unregistering dispatchers, 310
unsupported characters, 371

updating
Cognos 8 Go! Office, 82, 240
java environment, 131, 298, 316
Upfront
migrating content to Cognos 8, 45
upgrade
Series 7 secured PowerCube, 85
upgrading
affect on Chinese, Japanese, or Korean characters, 384
changes in product behavior, 17
Cognos 8, 58
Cognos 8 Go! Office, 81
Cognos 8 on an application server, 311
content store, 376
from Metrics Manager, 49
from other Cognos products to Cognos 8, 43
from ReportNet, 49
from Series 7, 49, 54
in an environment that includes Cognos 8 Controller, 58
Metric Designer projects, 57, 190
Metrics Manager, 72
Metrics Manager and security information, 73
metric store, 57, 155, 175
planning the move from test to production environment, 53
preparation, 50
problems with cryptographic keys, 388
published Cognos Series 7 PowerCubes, 80
ReportNet, 55
ReportNet to Cognos 8, 66
resources, 50
third-party products, 77
unable to uninstall ReportNet Service, 79
using silent configuration, 72
URI
changing, 196
default configuration settings, 104
User account
requirements to run the Cognos 8 service, 145
user credentials
changing in unattended configuration, 358
user interface
customizing language support, 221
mapping for product locale, 227
user locale
mapping to content locale, 225
User lookup property
special characters for LDAP namespace, 268
users
changing for Cognos Content Database, 194
definition, 403
UTF-8
encoding for email messages, 228

V

versions
supported ReportNet upgrades, 55
virtual directories
Cognos 8, 132
Cognos 8 Go! Office, 237
virtual machines, 313
virtual servers
configuring for Cognos 8, 132

W

WAR files, *See* Web archive files
Web aliases
Cognos 8, 132
Cognos 8 Go! Office, 237
Web archive files
deploying Cognos 8, 361
Web browser
workflow for configuring on client computers, 90
Web browsers
configuring, 135
errors in starting the Web portal, 381
errors when starting the web portal, 378
security settings, 94
WebLogic
application server, 304, 309
could not deserialize context attribute, 383
deploying p2pd.war file, 384
servlet class fails to load, 396
startup script, 301
startup script fails, 382
WebLogic 8
problem configuring SSL, 380

Web server
workflow for configuring on the gateway computer, 89
Web servers, 32, 35, 42
configuring, 132
enabling SSL, 133
MIME types for Cognos 8 Go! Office, 238
servlet gateways, 233
setting Report Studio load time, 132
single signon using Active Directory and IIS Web server, 262
WebSphere
application server, 303
single signon using application server, 252
WebSphere Application Server
Cognos 8 deployment failure, 382
deploying Cognos 8, 394
startup script fails, 382
Windows
system requirements, 93
Windows event log
destination for log messages, 217
Windows IIS
recommended gateway settings, 395
Windows integrated authentication, 262
Windows native security (NTLM)
enabling single signon, 287
using for authentication, 286
Windows Vista
affect on upgrade, 58
requirements for file locations, 150, 165, 169, 173
won character, 223
workflows
installation and configuration, 87

Y

yen character, 223